GFI Product Manual

GFI EventsManager™

Event log monitoring, management and archiving

User Manual

http://www.gfi.com

info@gfi.com

The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. GFI makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document.

If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.

All product and company names herein may be trademarks of their respective owners.

GFI EventsManager is copyright of GFI SOFTWARE Ltd. - 1999-2011 GFI Software Ltd. All rights reserved.

Document Version: ESM-UM-EN 2.03.02

Last updated: July 26, 2011

Contents

1 Introduction 5

1.1 About this manual 5
1.2 Conventions used in this manual 6
1.3 About GFI EventsManager 7
1.4 Key Features 8
1.5 How does GFI EventsManager work? 11
1.6 Navigating the GFI EventsManager management console 13

2 Getting Started 15

2.1 Introduction 15

3 Installation 19

3.1 Introduction 19
3.2 System requirements 22
3.3 Upgrading from a previous version 24
3.4 Installation procedure 25
3.5 What to do next 27

4 Event browsing 35

4.1 Introduction 35
4.2 Event filter/query builder 37
4.3 Event color-coding options 41
4.4 Event finder tool 43
4.5 Export events tool 43
4.6 Rule finder tool 47
4.7 Customizing the event viewer pane 48
4.8 Event maintenance 49

5 Generating reports 53

5.1 Introduction 53
5.2 Daily Digest 53
5.3 Settings report 55
5.4 Rules report 56
5.5 Operational history 58
5.6 Activity overview 59
5.7 Download the GFI EventsManager ReportPack 61
5.8 Launching the GFI EventsManager ReportPack 62

6 Manage event sources 65

6.1 Introduction 65
6.2 Managing event sources groups 65
6.3 Adding event sources 69
6.4 Configuring event source properties 70
6.5 Microsoft SQL Server sources 76
6.6 Oracle Server sources 80
6.7 Adding GFI LANguard event sources 89
6.8 Adding GFI EndPointSecurity event sources 91

7 Using event processing rules 93
7.1 Introduction 93
7.2 How event processing works 94
7.3 Collecting events 95
7.4 Archiving events 108
7.5 Select event processing rules 109
7.6 Triggering event source scanning manually 110

8 Manage rule-sets 112
8.1 Introduction 112
8.2 Managing rule set folders 113
8.3 Create log rules 114
8.4 Advanced event filtering parameters 131

9 Customizing alerts and actions 133
9.1 Introduction 133
9.2 Configuring default classification actions 134
9.3 Configuring alerting options 135

10 Configuring users and groups 143
10.1 Introduction 143
10.2 Manage user accounts 143
10.3 Manage groups 149
10.4 Manage console security 150

11 Status monitoring 159
11.1 Introduction 159
11.2 General status view 159
11.3 Job activity view 165
11.4 Statistics view 167

12 Database Operations 169
12.1 Introduction 169
12.2 Why database maintenance? 169
12.3 Create maintenance jobs 171
12.4 Create new anonymization job 183
12.5 Edit existing maintenance jobs 185

13 Miscellaneous 189
13.1 Enabling permissions on event sources manually 189
13.2 Setting permissions on target computers automatically via GPO 202
13.3 Disable UAC to scan target machines 206
13.4 Command line operations 206
13.5 Auto updating GFI EventsManager 211
13.6 Product licensing 213
13.7 Version information 215

14 Troubleshooting 217
14.1 Introduction 217
14.2 Common issues 217

14.3 Knowledge Base 220
14.4 Web Forum 220
14.5 Request technical support 220
14.6 Build notifications 221

15 Glossary 223

Index 227

List of tables

Table 1 - Quick Launch Console options 34
Table 2 - Export to HTML options 45
Table 3 - Add/Edit Template Options 47
Table 4 – Settings report heading information 55
Table 5 – Rules report heading information 56
Table 6 – Operational history reports 58
Table 7 – Export operational history options 59
Table 8 – Activity overview headings 59
Table 9 – Export operational history options 60
Table 10 - Event source group options 66
Table 11 - Synchronization properties - General tab 67
Table 12 - Example of synchronizations 67
Table 13 - Auditing options 74
Table 14 - Microsoft SQL Database group - General tab 76
Table 15 - Microsoft SQL Database group - Logon Credentials 76
Table 16 - Microsoft SQL Database group -SQL Server Audit 77
Table 17 - Microsoft SQL Database group - Settings 77
Table 18 - Microsoft SQL Database - General tab options 79
Table 19 - Microsoft SQL Database - Connection Settings tab 79
Table 20 - Microsoft SQL Database - Settings tab options 80
Table 21 - Oracle Database group - General tab 82
Table 22 - Oracle Database group - Oracle Audit 83
Table 23 - Oracle Database - General tab options 85
Table 24 - Oracle Database - General tab options 86
Table 25 - Oracle Database - Audit by Objects 87
Table 26 - Oracle Database - Audit by Statements 89
Table 27 - Rule-set folders available in GFI EventsManager 112
Table 28 - Parameters available in the Event ID field 131
Table 29 - Parameters available in the Source, Category and User fields 131
Table 30 - Parameters available in the Message and Process fields 131
Table 31 – Database alerts options 141
Table 32 - Move to database - Rollover options 175
Table 33 – Auto update options 212
Table 34 - Terms used in this manual 223

List of screenshots

Screenshot 1 - The GFI EventsManager management console 13
Screenshot 2 - Windows event log 16
Screenshot 3 - Customer and License detail screen 25
Screenshot 4 - Logon information screen 26
Screenshot 5 - Database backend alert displayed on Quick Start Dialog 27
Screenshot 6 - Database Options - Change database tab 28
Screenshot 7 - SQL Server Management - Logins folder 29
Screenshot 8 - SQL Server Management - Login Properties dialog 29
Screenshot 9 - Quick Start Dialog 30
Screenshot 10 - Events processed from local machine 31
Screenshot 11 - Select the type of event source 32
Screenshot 12 - Select computers from result 32
Screenshot 13 - Process events from selected machines 33
Screenshot 14 - GFI EventsManager Quick Launch Console 34
Screenshot 15 - GFI EventsManager: Events Browser 35
Screenshot 16 - Event details provided in the Events Browser 36
Screenshot 17 - Configure auto-refresh 37
Screenshot 18 - Selecting a filter 37
Screenshot 19 - GFI EventsManager: Events Browser 38
Screenshot 20- Custom query builder 39
Screenshot 21 - Query builder for an existing query 40
Screenshot 22 - Create new query using the query builder 40
Screenshot 23 - Default and custom event queries 41
Screenshot 24 - Color coding configuration 41
Screenshot 25 - Assigning event color-codes 41
Screenshot 26 - Advanced Color Filter 42
Screenshot 27 - Event finder tool 43
Screenshot 28 - Export events tool 44
Screenshot 29 - Export to HTML 44
Screenshot 30 - Export to HTML dialog box 44
Screenshot 31 - HTML Report Sample 45
Screenshot 32 - Add new template 46
Screenshot 33 - Define Template 46
Screenshot 34 - Find rule 48
Screenshot 35 - Customize view: columns 48
Screenshot 36 - Customize view 49
Screenshot 37 - Backup events dialog box 50
Screenshot 38 - Add a new database from the switch database dialog 50
Screenshot 39 - Clear all events dialog box 51
Screenshot 40 - Daily Digest email settings 54
Screenshot 41 - Daily digest email 54
Screenshot 42 – Generate configuration report 55
Screenshot 43 – Settings report sample 56
Screenshot 44 – Generate configuration report 57
Screenshot 45 – Generate configuration report 57
Screenshot 46 – Operational history report 58
Screenshot 47 – Operational history dialog 58
Screenshot 48 – Operational history report sample 59
Screenshot 49 – Activity overview button 60
Screenshot 50 – Activity overview dialog 60
Screenshot 51 – Activity overview report sample 61
Screenshot 52 - Downloading GFI EventsManager ReportPack 61
Screenshot 53 - Launching the GFI EventsManager ReportPack 62
Screenshot 54 - GFI EventsManager ReportPack console 62
Screenshot 55 - Add new event source group 65
Screenshot 56 - Synchronization properties - General tab 67
Screenshot 57 - Synchronization properties - Exclusion tab 68
Screenshot 58 - Synchronization properties -Schedule tab 68
Screenshot 59 - Configuration wizard: Specify the computers that will be monitored 69
Screenshot 60 - Browse the network for connected computers 70
Screenshot 61 - Group type 70
Screenshot 62 - Event sources properties dialog 71
Screenshot 63 - Configuring alternative logon credentials 72

Screenshot 64 - Specify operational time 73
Screenshot 65 - GFI EventsManager audit 74
Screenshot 66 - Event-processing configuration tabs 75
Screenshot 67 - Database Servers Groups 76
Screenshot 68 - Microsoft SQL Database group - SQL Server Audit tab 77
Screenshot 69 - Add new Microsoft SQL server 78
Screenshot 70 - Microsoft SQL Database - General tab 78
Screenshot 71 - Microsoft SQL Database - Connection Settings tab 79
Screenshot 72 - Microsoft SQL Database - Settings tab 80
Screenshot 73 - Database Servers Groups 81
Screenshot 74 - Oracle Database group - General tab 82
Screenshot 75 - Oracle Database group - Oracle Audit tab 83
Screenshot 76 - Add new Oracle server 84
Screenshot 77 - Oracle Database - General tab 85
Screenshot 78 - Oracle Database - Connection Settings tab 86
Screenshot 79 - Oracle Database -Audit by objects tab 87
Screenshot 80 - Oracle Database -Audit by statements tab 88
Screenshot 81 - Event generated by GFI LANguard 90
Screenshot 82 - Event generated by GFI EndPointSecurity 92
Screenshot 83 - Rule-sets folder and Rule-sets 93
Screenshot 84 - Log processing, classification and actions flowchart 94
Screenshot 85 - Computer group properties: Configuring logs to be processed 95
Screenshot 86 - Computer group properties: Configuring Windows Event Logs parameters 96
Screenshot 87 - Selecting the events to be collected 97
Screenshot 88 - Computer group properties: Configuring W3C event processing parameters 98
Screenshot 89 - Add a new W3C folder path 98
Screenshot 90 - Computer group properties: Syslog processing parameters 99
Screenshot 91 - Configuring Syslog Server 101
Screenshot 92- Syslog server properties 102
Screenshot 93 - Computer group properties: SNMP processing parameters 103
Screenshot 94 - Configuring SNMP Traps 104
Screenshot 95- SNMP Traps options 105
Screenshot 96 - Custom event logs setup 106
Screenshot 97 - Custom event logs dialog 107
Screenshot 98 - List of custom events 107
Screenshot 99 - Archiving events after processing 108
Screenshot 100 - Configure file folder 109
Screenshot 101 - Computer group properties: Configuring Windows Event Logs parameters 109
Screenshot 102 - Selecting event processing rules/rule-sets 110
Screenshot 103 - Triggering log collection manually 111
Screenshot 104 - The log type drop-down list 113
Screenshot 105 - New rule-set dialog box 114
Screenshot 106 - Selecting log-type from the provided drop-down 114
Screenshot 107 - GFI EventsManager: Select the Log(s) 115
Screenshot 108 - GFI EventsManager: Select the filtering conditions 115
Screenshot 109 - New processing rule wizard: Select event occurrence and importance 116
Screenshot 110 - New processing rule wizard: Select action 117
Screenshot 111 - New processing rule wizard: Select W3C Log 118
Screenshot 112 - New processing rule wizard: Configure filtering conditions. 118
Screenshot 113 - Edit filter rules 119
Screenshot 114 - New processing rule wizard: Select event occurrence and importance 119
Screenshot 115 - New processing rule wizard: Select action 120
Screenshot 116 - New processing rule wizard: Configure Conditions 121
Screenshot 117 - New processing rule wizard: Select event occurrence and importance 121
Screenshot 118 - New processing rule wizard: Select action 122
Screenshot 119 - New processing rule wizard: Configure Conditions 123
Screenshot 120 - New processing rule wizard: Select event occurrence and importance 123
Screenshot 121 - New processing rule wizard: Select action 124
Screenshot 122 - New processing rule wizard: Configure Conditions 125
Screenshot 123 - New processing rule wizard: Select event occurrence and importance 125
Screenshot 124 - New processing rule wizard: Select action 126
Screenshot 125 - Create rule from event 127
Screenshot 126 - New Rule dialog 127
Screenshot 127 -Updated conditions for the selected rule 128
Screenshot 128 - Edit an existing custom rule 129

Screenshot 129 - Log processing rule properties 130
Screenshot 130 - Available field operators 132
Screenshot 131 - Configuring default classification actions 134
Screenshot 132 - Default classification actions screen 135
Screenshot 133 - Configuring alerting options 136
Screenshot 134 - Alerting options dialog 137
Screenshot 135- Mail server properties dialog box 137
Screenshot 136- Format mail message 138
Screenshot 137 - Alerting Options: Network dialog box 138
Screenshot 138 - Alerting Options: SMS dialog box 139
Screenshot 139 - Alerting Options: SNMP dialog box 140
Screenshot 140 - Alerting Options: SNMP dialog box 141
Screenshot 141 - Configuring users and group's node 143
Screenshot 142 - Configuring the default EventsManagerAdministrator account 144
Screenshot 143 - EventsManager Administrator properties 145
Screenshot 144 - Configuring the typical working hours of an alert recipient 146
Screenshot 145 - Selecting alerts to be sent during and outside working hours 146
Screenshot 146 - Notification groups to which a user belongs 147
Screenshot 147 - Configuring GFI EventsManager administrator privileges 147
Screenshot 148 - GFI EventsManager new user privileges 148
Screenshot 149 - Groups configuration screen 149
Screenshot 150 - New groups setup 150
Screenshot 151 - Select the login options feature 151
Screenshot 152 - Login options dialog 151
Screenshot 153 - Login window 152
Screenshot 154 – Anonymization 153
Screenshot 155 – Anonymization options 154
Screenshot 156 - Select the Audit options feature 155
Screenshot 157 - Audit Options 156
Screenshot 158 - Auto-discovery credentials 157
Screenshot 159 - Dashboard View Options 159
Screenshot 160 - GFI EventsManager status: General view 159
Screenshot 161 - GFI EventsManager General Status view: Service Status 160
Screenshot 162 - GFI EventsManager General Status view: Important logon events 160
Screenshot 163 - GFI EventsManager General Status view: Critical and High importance events 161
Screenshot 164 - GFI EventsManager General Status view: Service Status 162
Screenshot 165 - GFI EventsManager Backup logs 163
Screenshot 166 - GFI EventsManager General Status view: Services Status 163
Screenshot 167 - GFI EventsManager General Status view: Network Activity 164
Screenshot 168 - GFI EventsManager Job Activity view 165
Screenshot 169 - GFI EventsManager Job Activity view: Active Jobs 165
Screenshot 170 - GFI EventsManager Job Activity view: Queued Jobs 166
Screenshot 171 - GFI EventsManager Job Activity view: Server Message History 166
Screenshot 172 - GFI EventsManager Job Activity view: Operational History 166
Screenshot 173 - GFI EventsManager Job Activity view: Job activity status 166
Screenshot 174 - GFI EventsManager Statistics view 167
Screenshot 175 - GFI EventsManager Statistics view: Events Count For Today 167
Screenshot 176 - GFI EventsManager Statistics view: Events count by log type 168
Screenshot 177 - GFI EventsManager Statistics view: Activity Overview 168
Screenshot 178 - Configuring Database Operations 171
Screenshot 179 - Database Operations Options dialog: GFI EventsManager unique identifier 172
Screenshot 180 - Database Operations Options dialog: Scheduling options 172
Screenshot 181 - New job wizard: Job Type dialog 173
Screenshot 182 - Data filter dialog: Specifying data filter conditions 174
Screenshot 183 - Specify when the job will be executed 174
Screenshot 184 - New job wizard: Move to database 175
Screenshot 185 - New job wizard: Export to file 176
Screenshot 186 - New job wizard: Export to file using encryption 177
Screenshot 187 - New job wizard: Import from file 178
Screenshot 188 - New job wizard: Import from file decryption 179
Screenshot 189 - New job wizard: Delete data 180
Screenshot 190 - Data filter dialog 181
Screenshot 191 - Creating a filter for Windows events: Edit filter dialog 182
Screenshot 192 - Advanced Filter settings 182
Screenshot 193 – New Decrypt/Re-encrypt database job wizard 183
Screenshot 194 – New anonymization job progress 184

Screenshot 195 - Viewing scheduled maintenance jobs 185
Screenshot 196 - Job activity status 186
Screenshot 197 - Editing a maintenance job 186
Screenshot 198 - Example dialog to edit a scheduled job 187
Screenshot 199 - Maintenance job priorities 187
Screenshot 200 - Firewall rules on Microsoft Windows XP 189
Screenshot 201 - Local security policy window 190
Screenshot 202 - Audit object access Properties 191
Screenshot 203 - Audit process tracking Properties 192
Screenshot 204 - Audit account management properties 193
Screenshot 205 - Audit system events properties 194
Screenshot 206 - Allowed programs in Microsoft Windows Vista or later 195
Screenshot 207 - Local security policy window 196
Screenshot 208 - Audit object access Properties 196
Screenshot 209 - Audit process tracking Properties 197
Screenshot 210 - Audit account management properties 198
Screenshot 211 - Audit system events properties 199
Screenshot 212 - Enable firewall rules in Microsoft Windows Server 2003 200
Screenshot 213 - Firewall rules on Microsoft Windows Server 2008 201
Screenshot 214 - Domain Policy console in Microsoft Windows Server 2003 202
Screenshot 215 - Group Policy Management in Microsoft Windows Server 2008 R2 203
Screenshot 216 - Group Policy Management Editor 204
Screenshot 217 - Predefined rules 205
Screenshot 218 - Predefined rules 206
Screenshot 219 - Auto update options 211
Screenshot 220 – Configure auto update 212
Screenshot 221 – Licensing page 213
Screenshot 222 - Update license key 213
Screenshot 223 - Register link 214
Screenshot 224 - Buy now! button 215
Screenshot 225 - Version Information screen 215

1 Introduction

1.1 About this manual

This user manual is a comprehensive guide aimed at assisting you in configuring and using GFI EventsManager.

This manual contains the following chapters:

CHAPTER	DESCRIPTION
Chapter 1	**Introduction** An overview of this manual and how GFI EventsManager works.
Chapter 2	**Getting Started** Describes how to install GFI EventsManager, including system requirements, pre-install actions required and how to upgrade from previous versions.
Chapter 3	**Installation** Shows how to configure GFI EventsManager for first time use, including how to configure the database backend and how to process event logs for the first time.
Chapter 4	**Event browsing** Explains how to use the built-in events browser to analyze events stored in the GFI EventsManager database backend, including: » Default event log queries and custom query builder » Event color-coding » Event finder tool.
Chapter 5	**Generating reports** Describes how to enable the GFI EventsManager ReportPack to create reports that further analyze the events stored in the GFI EventsManager database backend. In addition describes how to configure a user to receive GFI EventsManager Daily Digest email.
Chapter 6	**Manage event sources** Shows how to add and customize event sources to be monitored.
Chapter 7	**Using event processing rules** Explains how to use event processing rules.
Chapter 8	**Manage rule-sets** Describes how to create, edit and delete event processing rules.
Chapter 9	**Customizing alerts and actions** Shows how to set the alerts and actions that will be triggered on particular events.
Chapter 10	**Configuring users and groups** Explains how to configure alert recipient parameters including: » Personal details such as mobile phone number » Normal working hours » Type of alerts that will be sent to every recipient.
Chapter 11	**Status monitoring** Describes how to analyze the status of GFI EventsManager as well as view statistical information and processed events.
Chapter 12	**Database Operations** Explains how to centralize events collected by other remote GFI EventsManager instances and how to optimize database backend performance.

CHAPTER	DESCRIPTION
Chapter 13	**Miscellaneous** Describes miscellaneous options such as permissions, command line operations and licensing.
Chapter 14	**Troubleshooting** Explains what main sources of information are available to help administrators troubleshoot product issues.
Chapter 15	**Glossary** Defines technical terms used within GFI EventsManager.

1.2 Conventions used in this manual

The following table contains a description of the common terms and conventions used in this manual:

TERM	DESCRIPTION
	Additional information and references essential for the operation of GFI EventsManager.
	Important notifications and cautions regarding potential issues that are commonly encountered.
►	Step by step navigation instructions to access a function.
Bold text	Indicate a control within the user interface, such as nodes, menus and buttons.
<Italic text>	Replace text within angle brackets. Such as file paths and custom parameters.

For any technical terms and their definitions as used in this manual, refer to Glossary chapter in this manual.

1.3 About GFI EventsManager

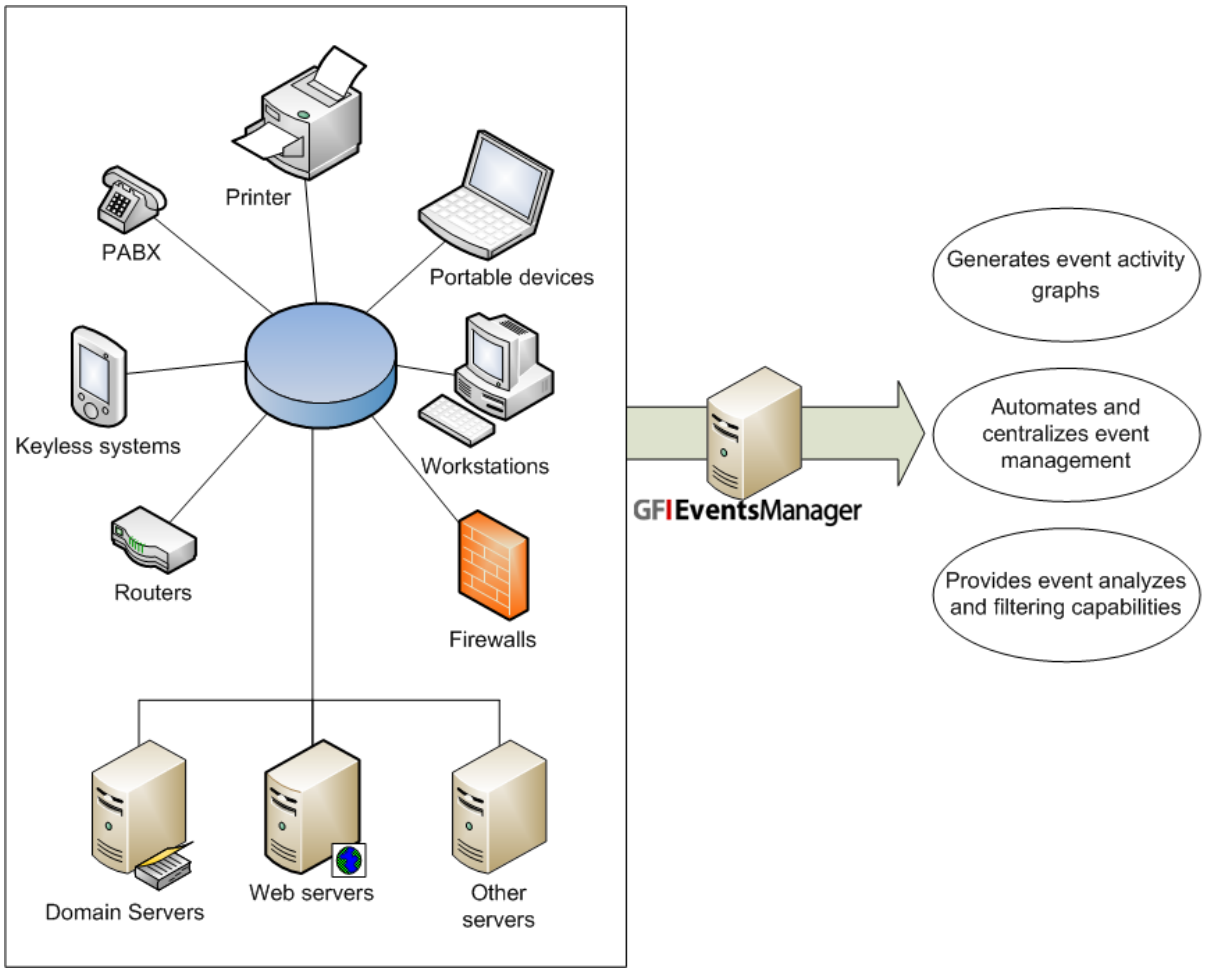


Figure 1 - GFI EventsManager integrates into any existing IT infrastructure

GFI EventsManager is a results oriented event log management solution which integrates into any existing IT infrastructure, automating and simplifying the tasks involved in network-wide events management.

Through the features supported by GFI EventsManager you can:

- Automatically collect W3C, Syslog, SNMP Traps and Windows event logs from network devices and Windows/Linux/Unix based systems and manage them through one console.
- Archive collected events in a centralized SQL Server based database backend for future analysis and forensic studies.
- Automatically transfer events from the database to external files.
- Filter unwanted events and classify key events through the use of powerful default or custom-built event processing rules.
- Automate alerting and remedial actions such as the execution of scripts and files on key events.
- Monitor your network activity and the status of your GFI EventsManager scanning engine through a built-in graphical dashboard.
- Analyze events through a built-in events browser as well as export these events to CSV files for further processing and report customization.
- Simplify event forensics through specialized tools which include a built-in event query builder, an event finder tool and an event color-coding tool.
- Increase event processing power through a high-performance event scanning engine.
- Generate, schedule as well as email event activity and trend reports through GFI EventsManager ReportPack - the powerful reporting companion tool which ships by default with GFI EventsManager.

- Monitor the operational health status of your SQL Servers in real-time by processing the activity logs/messages generated by day-to-day SQL Server operations.
- Monitor Oracle database servers. GFI EventsManager collects and process events generated by Oracle Relational database management systems.
- Protect data contained in event logs so that confidential information can be encrypted and viewed only by authorized personnel.

1.4 Key Features

Extended event log support

GFI EventsManager is able to process various event log types including Windows Event Logs, W3C logs, Syslog and SNMP Trap messages. This allows you to collect more data from the different hardware and software systems that are most commonly available on a typical corporate network. For a summary list of hardware and software systems that are supported by GFI EventsManager out of-the-box refer to:

http://kbase.gfi.com/showarticle.asp?id=KBID003302.

Rule-based event log management

GFI EventsManager ships with a pre-configured set of event processing rules that allow you to filter and classify events collected from a variety of event-log sources. You can run these default rules without performing any configuration or you can choose to customize these rules or create tailored ones that suite your network infrastructure. For a list of event-log sources that can be processed by GFI Events out-of-the-box refer to:

http://kbase.gfi.com/showarticle.asp?id=KBID002868.

Event log scanning profiles

GFI EventsManager enables you to organize event log scanning rules into **Scanning Profiles**. In a scanning profile, you can configure the set of event log monitoring rules that will be applied to a specific computer or group of computers. The benefits of these profiles include:

- The simplification product administration tasks by providing a centralized way of tuning event processing rules.
- Allowing administrators to create different sets of event log rules that suit the roles of scanned event sources and the corporate network environment. For example, you can setup a set of rules which apply only to workstations in a particular department.

Allow granular configuration of rules

Administrators can create an event processing profile that is generic for all computers and a number of separate profiles which complement the generic profile by providing additional and more specialized event log rules on a computer by computer basis.

Translates cryptic Windows events

One major drawback of Windows Event Logs is that they are not user friendly - too cryptic for the user to understand. In fact this is one of the main reasons why only few administrators really peer into Windows Event Logs. GFI EventsManager overcomes this problem by translating event descriptions into a way that is more users friendly and easier to understand.

Enhanced event scanning engine

GFI EventsManager includes an event scanning engine that has been tuned to effectively speed up event scanning for maximum performance. This engine adopts a plug-in based

concept that allows the plugging-in of additional features/modules without having to perform physical changes to the existing code - hence more stability without effecting scalability.

Automatic noise reduction

GFI EventsManager identifies and removes unwanted event data (such as noise and background process generated events) providing you with only the relevant, usable data. Hence facilitates event forensics by reducing the amount of events to be analyzed.

Enhanced real-time actions

GFI EventsManager can generate alerts or trigger actions such as script execution when key events are detected. You can alert one or more people in various ways including: email, network messages, and SMS notifications sent through an email-to-SMS gateway or service. Actions can be configured to trigger on event classification or by configuring specific conditions in event processing rules.

Advanced event filtering features

GFI EventsManager ships with a number of event filtering features including:

- Pre-configured event queries and a custom event query builder: The pre-configured event queries allow you to sift event log data and browse only the required events - without deleting any records from your database backend. The built-in event query builder allows you to create your own custom event queries.
- Event color-coding capabilities: Through this feature you can selectively color particular events in specific colors. This way during log browsing you can easily identify important events through their color.
- Event finder tool: With this tool you can quickly locate important events by providing specific search criteria such as event type.

Event centralization

GFI EventsManager enables you to monitor and manage events generated by Windows\Linux\Unix systems, network devices and software applications through a single user console.

User access privileges

GFI EventsManager enables you to assign management console access privileges on a user-by-user basis. This means that you can allow specific users to access the GFI EventsManager console for event-browsing only and at the same time allow other more privileged users to access and change the GFI EventsManager configuration settings.

SQL Server audit

GFI EventsManager enables you to automatically monitor the operational health status of your SQL Servers. This is achieved by processing in real-time the activity logs/messages generated by day-to-day SQL Server operations. SQL server activity that is monitored includes server startup, login activity, backups, server-side traces and more. Additionally, GFI EventsManager can also alert you via email, network or SMS notifications on key events like server shutdown and consecutive failed logins.

Oracle Server audit

GFI EventsManager enables you to automatically monitor the activity and the operational health status of your Oracle Servers. Within GFI EventsManager you can configure Oracle servers to log audit events. Oracle audit events are stored in a specific table on the Oracle server. GFI EventsManager collects and process these events. GFI EventsManager can also alert you via email, network or SMS notifications when specific events occur.

Database operations (WAN Connector)

The Database Operations module enables you to collect events data from GFI EventsManager installations on multiple sites and locations across your network into a central database. This add-on integrates and centralizes events collected and processed and allows you to backup/restore events on demand. Through Database Operations you can manage the size of the database - without the need for manual intervention - not only through centralization but by also being able to export events and back them up as needed.

Management Information Base

Management Information Base (MIBs) contains definitions and device information that are provided by device manufacturers. GFI EventsManager ships with MIB definitions for the following vendors: Cisco, 3Com, IBM, HP, Check Point, Alcatel, Dell, Netgear, SonicWall, Juniper Networks, Arbor Networks, Oracle, Symantec, Allied Telesis and others. GFI EventsManager also allows you to edit the MIB tree.

1.5 How does GFI EventsManager work?

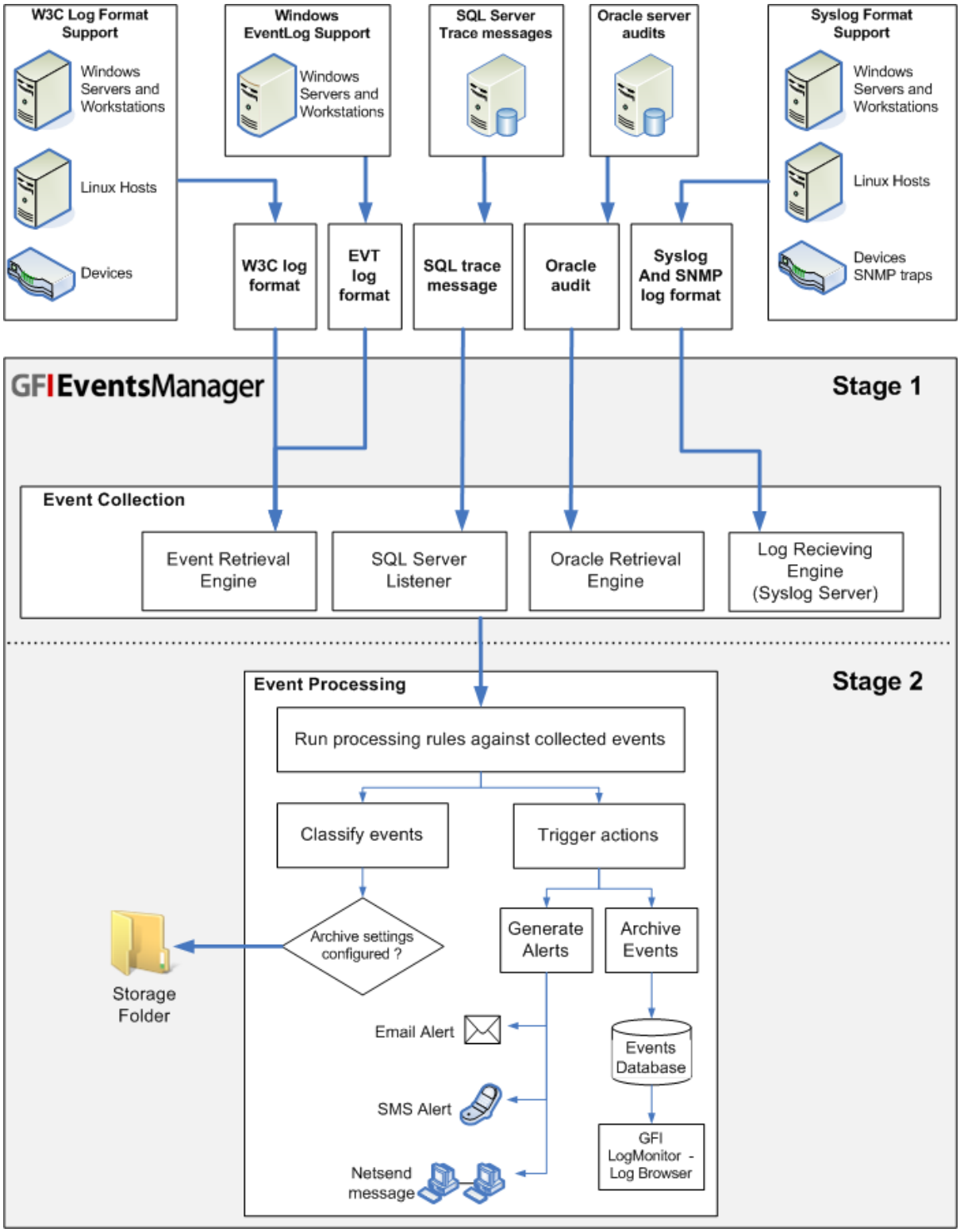


Figure 2 - The GFI EventsManager operational stages

The operational functionality of GFI EventsManager is divided into 2 stages:

» **Stage 1**: Event Collection

» **Stage 2**: Event Processing

1.5.1 Stage 1: Event Collection

During the Event Collection stage, GFI EventsManager collects logs from specific event sources. This is achieved through the use of 2 event collection engines: The Event Retrieval Engine and the Event Receiving Engine.

The Event Retrieval Engine

The Event Retrieval Engine is used to collect Windows Event Logs and W3C logs from networked event sources. During the Event Collection process this engine will:

1. Log-on to the event source(s)

2. Collect events from the source(s)

3. Send collected events to the GFI EventsManager Server

4. Log-off from the event source(s).

The Event Retrieval Engine collects events at specific time intervals. The event collection interval is configurable from the GFI EventsManager management console

The SQL Server Listener

The listener receives trace messages from the scanned Microsoft SQL Server in real time. On receipt, EventsManager processes the message immediately.

The Oracle Retrieval Engine

The Oracle Retrieval Engine connects periodically to Oracle servers and collects audits from a specific auditing table. Similar to the Microsoft Windows Event Retrieval Engine, GFI EventsManager processes events generated by the Oracle server.

Log Receiving Engine

The Event Receiving Engine acts as a Syslog and an SNMP Traps server; it listens and collects Syslog and SNMP Trap events/messages sent by various sources on the network. As opposed to the Event Retrieval Engine, the Event Receiving Engine receives messages directly from the event source; therefore it does not require to remotely log-on to the event sources for event collection. Further to this, Syslog and SNMP Trap events/messages are collected in real-time and therefore no collection time intervals need to be configured.

By default, the Event Receiving Engine listens to Syslog messages on port 514 and to SNMP Trap messages on port 162. Both port settings are however customizable via the GFI EventsManager management console.

1.5.2 Stage 2: Event Processing

During this stage, GFI EventsManager will run a set of Event Processing Rules against collected events. Event Processing rules are instructions that:

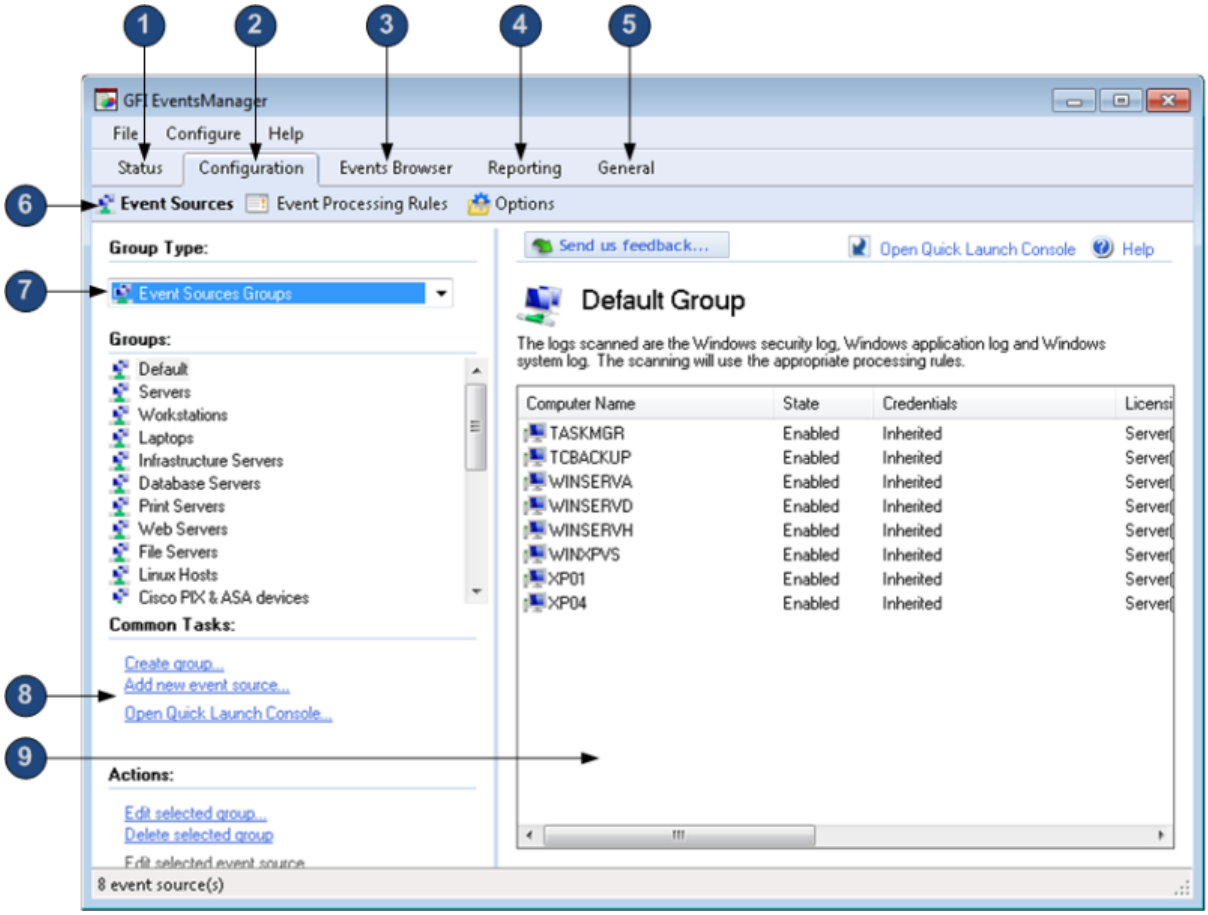
- Analyze the collected logs and classify processed events as Critical, High, Medium, Low or Noise (unwanted or repeated events)
- Filter events that match specific conditions
- Trigger email, SMS and network alerts on key events
- Trigger remediation actions such as the execution of executable files or scripts on key events
- Optionally archive collected events in the database backend.

GFI EventsManager can be configured to archive events without running Event Processing rules. In such cases, even though no rules will be applied against collected logs, archiving will still be handled by the Event Processing stage.

After processing the rules, GFI EventsManager can be configured to store the collected events in a storage folder. The administrator can configure the path of the storage folder and configure which events are stored. This function will minimize database growth, and allows the administrator to store only important events in the database.

Some of the key modules in GFI EventsManager must run under administrative privileges. For more information on these modules refer to: http://kbase.gfi.com/showarticle.asp?id=KBID001122.

1.6 Navigating the GFI EventsManager management console



Screenshot 1 - The GFI EventsManager management console

SECTION	DESCRIPTION
1	**Status option** - Use this option to view the status of GFI EventsManager and statistical information on processed logs.
2	**Configuration option** - Use this option to access and configure the main event processing options.
3	**Events Browser** - Use this option to browse the events stored in the GFI EventsManager database backend.
4	**Reporting** - Use this option to download and install the GFI EventsManager ReportPack.
5	**General options** - Use this option to check for product updates, as well as view version and licensing details.
6	**Tab options** - Use the Tab options to access and configure GFI EventsManager operational parameters.
7	**Group Type** - Use this drop-down to switch between event log source groups (i.e. Computer and Database Servers Groups).
8	**Left pane** - Use this pane to navigate through the additional configuration options provided in GFI EventsManager.
9	**Right pane** - Event browsing and parameter configuration pane.

2 Getting Started

2.1 Introduction

What is a computer log?

A computer log is a collection of event entries. These entries provide an audit trail of information related to the activity of a network or computer system. In fact, computer logs are recorded in a certain scope to provide information suitable for forensic analysis. The computer log may be a binary file as in the case of Windows logs, or text-based files as in the case of Syslog or W3C logs.

Such events include various details such as the date and time the event occurred and a related description. Event entries are often stored in chronological order to facilitate event browsing and forensic analysis.

What are Windows Event Logs?

Windows Event Logs are a systematic recording of computer related events that occurred within computer systems and networks running on Windows Operating Systems. In systems running on Windows 2000/XP/2003/VISTA, events are recorded and organized in 3 default event logs:

- **Application log**
- **Security log**
- **System log.**

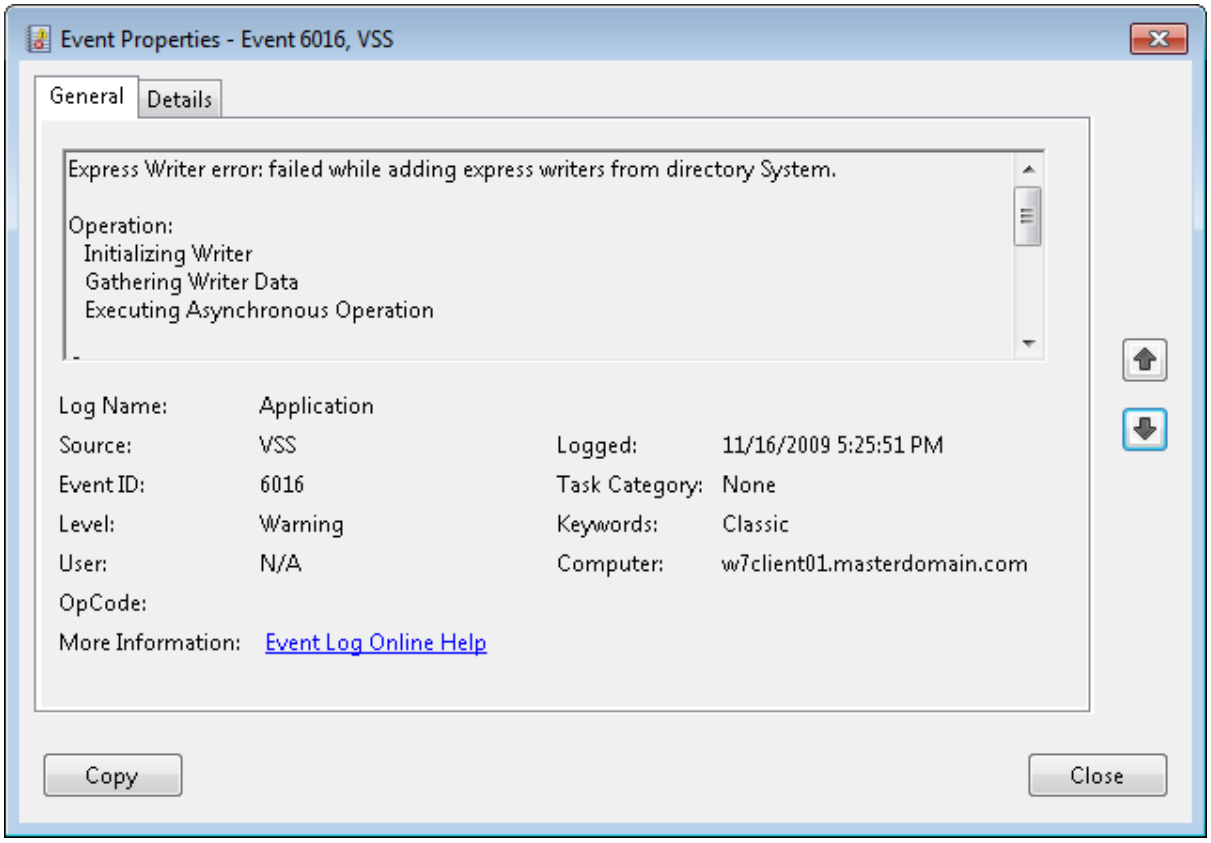
Computers with specialized network roles such as domain controllers and DNS servers allow the logging of events to additional (default) logs such as:

- **Directory service log**
- **File Replication service log**
- **DNS server log.**

Windows Event Logs contain the following types of events:

- **Error** - Error events indicate that a significant problem, such as loss of data or functionality has occurred. For example an Error event is recorded every time that a service or driver fails to load during startup.
- **Warning** - Warnings indicate events that are not necessarily significant, but which may possibly cause future problems. For example, a Warning event is recorded every time that disk space runs low.
- **Information** - Information events describe the successful operation of an application, driver, or service. For example, an Information event is recorded every time that a network driver loads successfully.
- **Success Audit** - Success audit events indicate security access attempts that were successful. For example, a Success Audit event is recorded every time that a user successfully logs on to his Windows based workstation.
- **Failure Audit** - Failure audit events indicate security access attempts that failed. For example, a Failure audit event is recorded every time that a user fails to access a network drive.

A sample of the information typically recorded in a Windows Event Log is shown below.



Screenshot 2 - Windows event log

What are W3C logs?

W3C logs are used mainly by web servers to log web related events including web logs. W3C logs are recorded in text-based flat files using any one of the two W3C logging formats currently available:

- W3C Common Log file format
- W3C Extended Log File format.

The W3C common log file format was the first format to be released and to date it is still the default format used by a variety of popular web servers including Apache. There is however one downside - the information about each server transaction is fixed and does not provide for certain important fields such as referrer, agent, transfer time, domain name, or cookie information. To overcome this problem, the W3C Extended log file format was released. This newer type of log is in customizable ASCII text-based format, permitting a wider range of data to be captured. The W3C Extended log file format is the default log file format used by Microsoft Internet Information Server (IIS).

A sample of the information typically recorded in a W3C extended type log is shown below.

```
#Version: 1.0

#Date: 04-Sep-2009 00:00:00

#Fields: time cs-method cs-uri

00:34:23 GET /WebSRV/Pg_Snippet.html

12:21:16 GET /WebSRV/ Button_pg.html

12:45:52 GET /WebSRV/ Login_Pg.html

12:57:34 GET /WebSRV/ Error_msg.html
```

What are Syslogs?

Syslog is the standard for logging messages, such as system events, in an IP network. The Syslog standard is most commonly used for the logging of events by computer systems running on UNIX and Linux as well by network devices and appliances such as Cisco routers and the Cisco PIX firewall. Syslog events are not directly recorded by applications running on the computer systems. Whenever an event is generated, the respective computer will send a small textual message (known as Syslog message) to a dedicated server commonly known as 'Syslog server'. The Syslog server will then save the received message into a log file. Syslog messages are generally sent as clear text; however, an SSL wrapper can be used to provide for a layer of encryption.

Syslog is typically used for computer system management and security auditing. While it has a number of shortcomings, its big plus is that Syslog is supported by a wide variety of devices and receivers. Because of this, Syslog can be used to integrate log data from many different types of systems into a central repository using the Syslog server as a log aggregator.

The Syslog daemon handles the recording of Syslog messages/events in log files. The Syslog message is composed of two main parts:

1. The 'header' which contains date/time information as well as the IP or computer name from where the message has originated.

2. The "message" which includes the program or subsystem name and the message itself, separated by a colon. The following is an example of a Syslog message:

```
Sep 4 10:10:10 10.245.2.11 foo[421]: this is a message from WebSRV
```

What are SNMP Traps?

SNMP Traps are used by network management systems to monitor network devices (such as routers, firewalls or switches) for conditions that require administrative attention. This includes monitoring device uptime, inventories of operating system versions and collecting interface information. SNMP enabled devices do not record event messages locally but instead these transmit event details to an SNMP Trap server which analyzes these occurrences and alert systems administrators on key events.

GFI EventsManager includes its own SNMP Trap server that captures SNMP messages and informs systems administrators of network device failures and other critical events. GFI EventsManager supports various versions of SNMP Traps including SNMP versions 1, 2 and 3 (the encoded version).

What are SQL Server audit logs?

Microsoft SQL Server generates event logs that allow the network administrator to monitor database activity. GFI EventsManager allows you to process the activity logs generated by day-to-day SQL Server operations such as server startup or on key events such as failed logons. Alerts can also be created when key events such as consecutive login failure is identified in Microsoft SQL Server audit logs.

What are Oracle Server audit logs?

Oracle Servers can be configured to generate event logs that enable administrators to monitor activity. GFI EventsManager can be configured to collect and process these events. Oracle Server auditing includes data related to:

- Data manipulation actions
- User access actions
- User privileges
- Database schema
- Database structure.

3 Installation

3.1 Introduction

Where can I install GFI EventsManager on my network?

GFI EventsManager can be installed on any computer which meets the minimum system requirements irrespective of the location on your network.

Use GFI EventsManager to manage the events generated:

» On the same computer where it is installed

» On all the computers that are reachable from the computer on which it is installed.

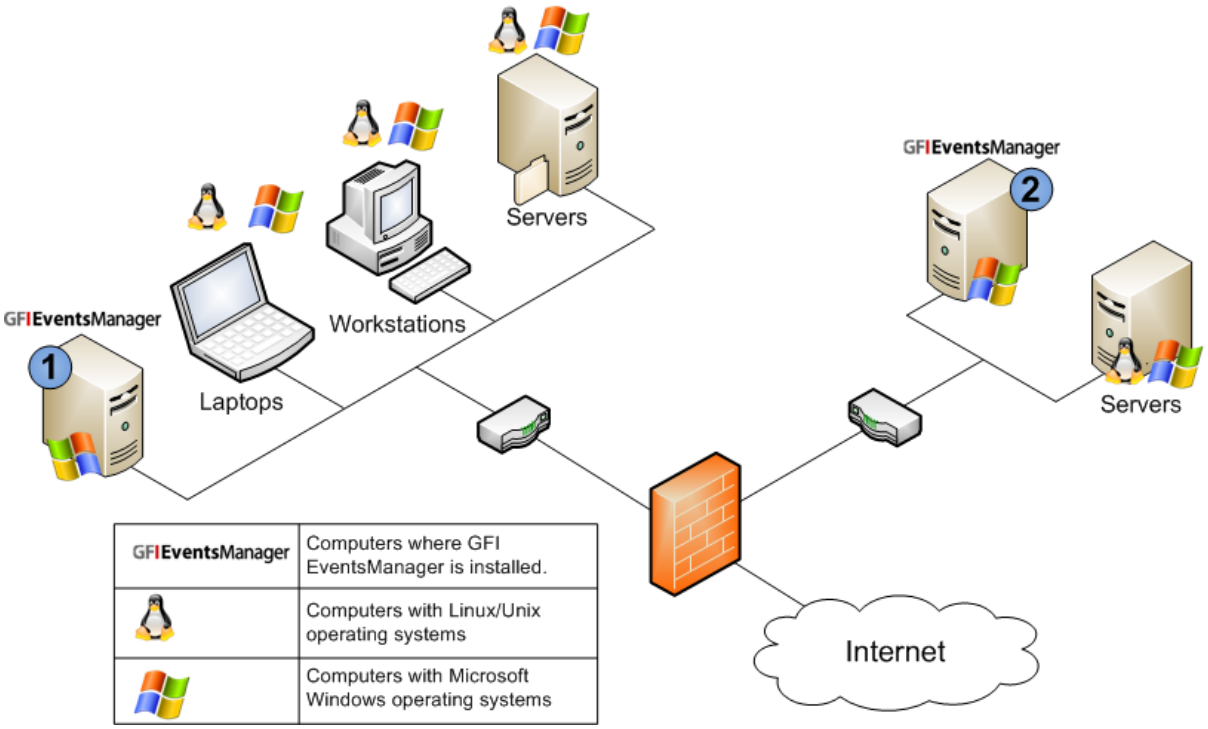


Figure 3 - GFI EventsManager deployment scenario

GFI EventsManager can be deployed:

1. In your network to monitor the activity of internal servers and workstations/end points.

2. On the DMZ to monitor and manage the events generated on your servers.

3.1.1 Deployment of GFI EventsManager on a local area network

GFI EventsManager can be deployed on Windows based networks as well as on mixed environments where Linux and UNIX systems are being used as well.

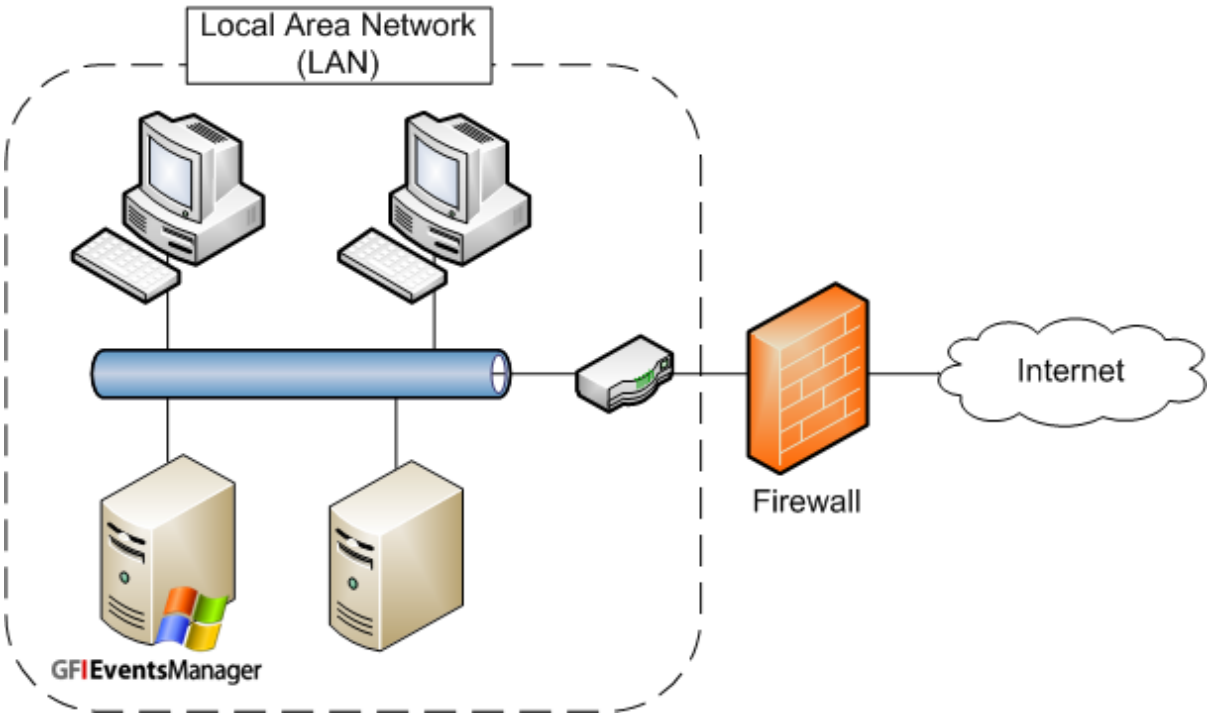


Figure 4 - Deployment of GFI EventsManager on LAN

When installed on a Local Area Network (LAN) GFI EventsManager can manage Windows events, W3C event logs, Syslog messages, SNMP Trap and SQL Server audit messages generated by any hardware or software that is connected to the LAN, including:

- Workstations and Servers (e.g. Apache web-servers)
- Network appliances (e.g. Cisco PIX firewalls)
- Third party software (e.g. GFI EndPointSecurity)
- Specialized Services (e.g. Microsoft Internet Information Server - IIS)
- PABXs, Keyless Access Systems, Intrusion detections systems and more.

When installed on a LAN, GFI EventsManager can also be used to collect events from hardware and software systems deployed on a Demilitarized Zone (DMZ). Since a firewall or a router usually protects this zone with network traffic filtering capabilities, you must make sure that:

1. The communication ports used by GFI EventsManager are not blocked by the firewall. For more information on the communication ports used by GFI EventsManager refer: http://kbase.gfi.com/showarticle.asp?id=KBID002770.

2. That GFI EventsManager has administrative privileges over the computers that are running on the DMZ.

3.1.2 Deployment of GFI EventsManager on a demilitarized zone

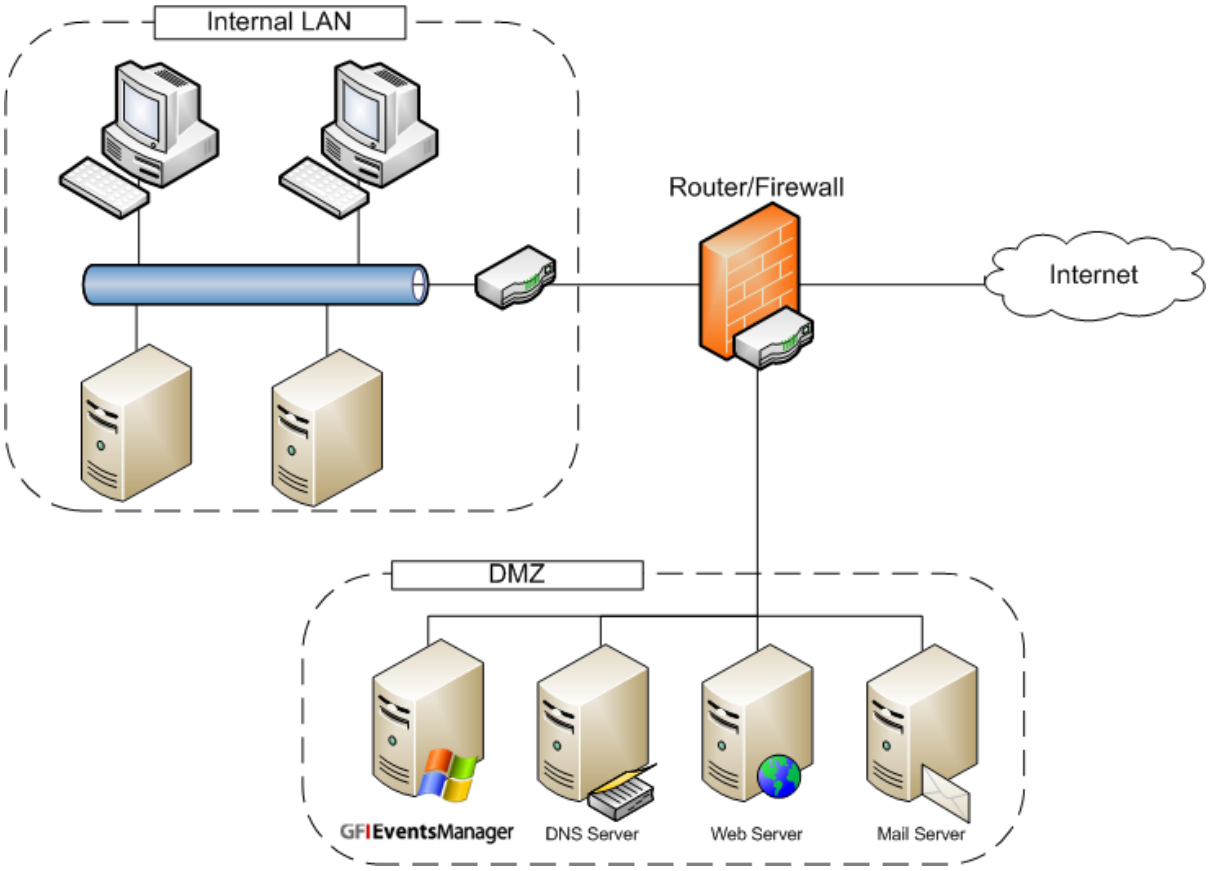


Figure 5 - The DMZ sits between the internal LAN and the Internet

GFI EventsManager can also be deployed on a Demilitarized Zone (DMZ). This is the neutral network which sits between the "internal" corporate network and the "outside world" (i.e. the internet). The deployment of GFI EventsManager on a DMZ helps you automate the management of events generated by DMZ hardware and software systems.

Automate management of Web and Mail server events

DMZ networks are normally used for the running of hardware and software systems that have internet specific roles such as HTTP servers, FTP servers, and Mail servers.

Hence, you can deploy GFI EventsManager to automatically manage the events generated by:

- Linux/Unix based web-servers including the W3C web-logs generated by Apache web-servers on LAMP web platforms.
- Windows based web-servers including the W3C web-logs generated by Microsoft Internet Information Servers (IIS).
- Linux/Unix and Windows based mail-servers including the Syslog auditing services messages generated by Sun Solaris v. 9 or later.

Automate management of DNS server events

If you have a public DNS server, there's a good chance that you are running a DNS server on the DMZ. Hence you can use GFI EventsManager to automatically collect and process DNS server events including those stored in your Windows' DNS Server logs.

Automate management of network appliance events

Routers and firewalls are two network appliances commonly found in a DMZ. Specialized routers and firewalls (e.g. Cisco IOS series routers) not only help protect your internal network, but provide specialized features such as Port Address Translation (PAT) that can augment the operational performance of your systems.

By deploying GFI EventsManager on your DMZ, you can collect the events generated by such network appliances. For example, you can configure GFI EventsManager to act as a Syslog Server and collect in real-time the Syslog messages generated by Cisco IOS routers.

3.2 System requirements

3.2.1 Hardware requirements

- Processor: 2.5 GHz dual core or higher
- RAM: 2GB
- Hard disk: 10 GB of available space

	Hard disk size depends on your environment, the size specified in the requirements is the minimum required to install and archive events.
	If Microsoft SQL Server is installed on the same machine as GFI EventsManager, consider using 1GB to 2GB more RAM than required.

3.2.2 Software requirements

Supported Operating Systems (x86 or x64)

- Windows Server 2008 - Standard or Enterprise
- Windows Server 2008 R2 – Standard or Enterprise
- Windows Server 2003 SP2 - Standard or Enterprise
- Windows 7 - Enterprise, Professional or Ultimate
- Windows Vista SP1 - Enterprise, Business or Ultimate
- Windows XP Professional SP3
- Windows SBS 2008
- Windows SBS 2003

Other components

- .NET framework 4.0
- Microsoft Data Access Components (MDAC) 2.8 or later
- (Optional) A mail server (If email alerting is configured)
- Microsoft SQL Server 2005 or later (including Microsoft SQL Express edition) for events archiving.

	Microsoft SQL server must have TCP port 1433 open to store events collected by GFI EventsManager. For more information, refer to http://support.microsoft.com/kb/287932
	Microsoft Data Access Components (MDAC) 2.8 can be downloaded from http://www.microsoft.com/Downloads/details.aspx?familyid=6C050FE3-C795-4B7D-B037-185D0506396C&displaylang=en

Event sources

The table below describes the configuration required for event sources:

LOG TYPE	DESCRIPTION
Windows event log processing	Enable remote registry.
W3C log processing	The source folders must be accessible via Windows shares
Syslog and SNMP Traps processing	Configure sources/senders to send messages to the computer/IP where GFI EventsManager is installed.
Scanning machines with Windows Vista or later	Install GFI EventsManager on a computer running Windows Vista or later.
System auditing	Enable auditing on event sources. For information on how to enable auditing, refer to Miscellaneous section in this manual.

3.2.3 Ports and permissions

Ports used by GFI EventsManager

The table below describes the ports used by GFI EventsManager to collect and process events.

PORT	PROTOCOL	DESCRIPTION
135	UDP and TCP	Target machines use this port to publish information regarding available dynamic ports. GFI EventsManager uses this information to be able to communicate with the target machines.
139 and 445	UDP and TCP	Used by GFI EventsManager to retrieve the event log descriptions from target machines.
162	UDP and TCP	Used by GFI EventsManager to receive SNMP traps. Ensure that this port is open on the machine where GFI EventsManager is installed
514	UDP and TCP	Used by GFI EventsManager to receive SYSLOG messages.
1433	UDP and TCP	Used by GFI EventsManager to communicate with the SQL Server database backend. Ensure that this port is enabled on Microsoft SQL Server and on the machine where GFI EventsManager is installed.
1521	UDP and TCP	Used to collect Oracle Server audit logs. Port 1521 is the default port for this connection. If the port is changed manually in the Oracle Listener's configuration, adjust firewall settings accordingly.
49153	UPD and TCP	Used by GFI EventsManager to collect events from event sources with Microsoft Windows Vista or Microsoft Windows 7.

Firewall permissions

When using Microsoft Windows firewall, enable all firewall permissions and policies listed in the table below:

FIREWALL PERMISSIONS AND AUDIT POLICIES	MICROSOFT WINDOWS SERVER 2008	MICROSOFT WINDOWS SERVER 2003	MICROSOFT WINDOWS XP	MICROSOFT WINDOWS VISTA	MICROSOFT WINDOWS 7
Remote Event Log Management	Enable	Not applicable	Not applicable	Enable	Enable
File and Printer sharing	Enable	Enable	Enable	Enable	Enable
Network discovery	Enable	Not applicable	Not applicable	Enable	Enable
Audit policy: Object access	Enable	Not applicable	Not applicable	Enable	Enable

FIREWALL PERMISSIONS AND AUDIT POLICIES	MICROSOFT WINDOWS SERVER 2008	MICROSOFT WINDOWS SERVER 2003	MICROSOFT WINDOWS XP	MICROSOFT WINDOWS VISTA	MICROSOFT WINDOWS 7
Audit policy: Process tracking	Enable	Not applicable	Not applicable	Enable	Enable
Audit policy: Audit account management	Enable	Enable	Enable	Enable	Enable
Audit policy: Audit system events	Enable	Enable	Enable	Enable	Enable

For more information how to set permissions refer to the following sections:

- To apply settings manually on each event source, refer to Enabling permissions on events sources manually
- To apply settings automatically on event sources using Microsoft Active Directory GPO, refer to Setting permissions on events sources automatically via GPO.

3.2.4 Microsoft Windows Vista and Microsoft Windows 7

Microsoft Windows Vista and Microsoft Windows 7 introduced extensive structural changes in event logging and event log management. The most important of these changes include:

- A new XML-based format for event logs. This provides a more structured approach to reporting on all system occurrences.
- Event categorization in four distinct groups: Administrative, Operational, Analytic and Debug
- A new file format (evtx) that replaces the old evt file format.

Due to these changes, to collect and process event logs from Microsoft Windows Vista or later, GFI EventsManager must be installed on a system running Microsoft Windows Vista or later. (For example, GFI EventsManager cannot be installed on Microsoft Windows XP to monitor events on Microsoft Windows 7 machines).

Windows XP events can be collected when GFI EventsManager is installed on Microsoft Windows Vista or later machines.

When GFI EventsManager is using a non-domain account to collect events from Microsoft Vista machines or later, target machines must have User Account Control (UAC) disabled. For more information on how to disable UAC, refer to Disable UAC to scan target machines section in this manual.

3.3 Upgrading from a previous version

Upgrading from version 8.x and retaining configuration settings is fully supported. Upgrading from version 7.x is possible but all configuration settings will be lost.

Upgrading from versions older than version 7 is not possible due to the underlying operational and processing technology subsystems which are different from the current version of GFI EventsManager. You will still however be able to run an older (pre-version 7) version of GFI EventsManager on the same machine on which a newer version of GFI EventsManager is installed since there are no conflicts between the older and the newer versions.

3.4 Installation procedure

GFI EventsManager includes an installation wizard which will assist you through the installation process. To start the installation:

1. Close all running applications and log-on the target computer using an account which has local administrative privileges.

2. Double-click GFI EventsManager setup file.

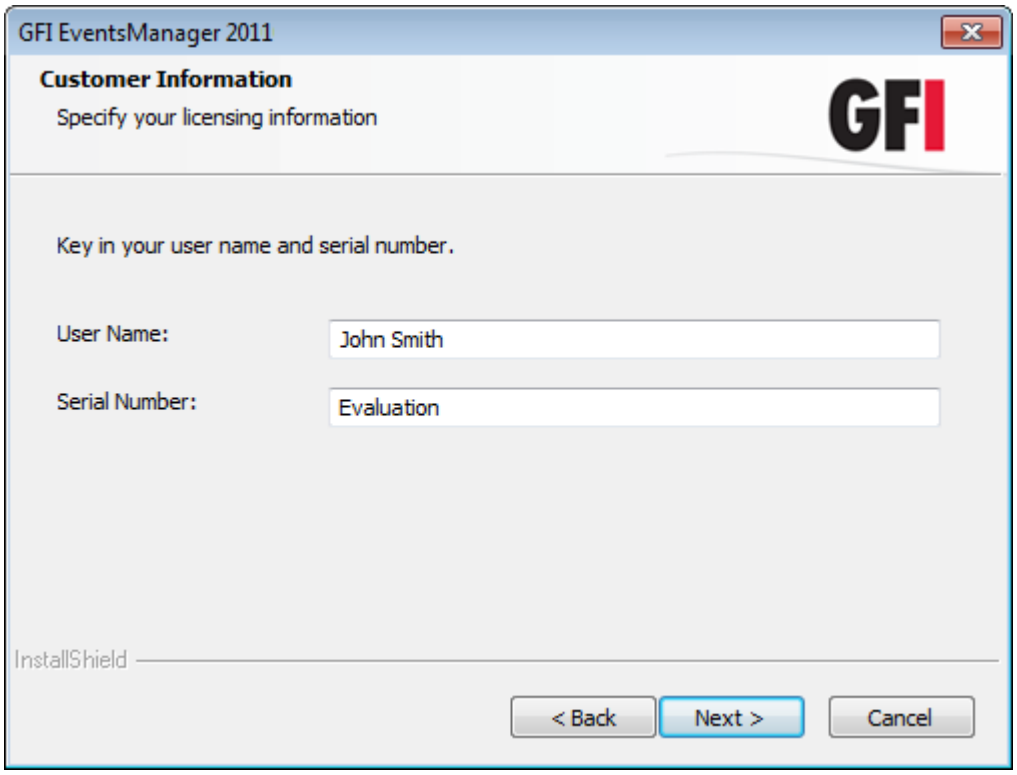
	If an older version of GFI EventsManager is detected, the wizard will enable you to retain or delete the GFI EventsManager configuration settings.
	If any pre-requisites are missing, the wizard will enable you to download and install all pre-requisites.

3. Click **Next**.

4. Read the licensing agreement carefully. Select '**I accept the Licensing agreement**' option and click **Next**.

5. If an installation of Microsoft SQL Server is not detected on the local machine, the **SQL Server Express install** is launched automatically. Select one of the following options:

- Download and install Microsoft SQL 2005 Express Edition
- Use a remote instance of Microsoft SQL Server.
- Click **Next**.



Screenshot 3 - Customer and License detail screen

6. Key-in your name and license key. If you are evaluating the product, leave the license key as default (example, '**Evaluation**') and click **Next**.

Screenshot 4 - Logon information screen

7. Key-in a user name and password of a domain administrator account and click **Next**.

8. Specify an alternative installation path or click **Install** to leave as default.

9. Click **Finish**.

For more information on launching GFI EventsManager for the first time, refer to Running GFI EventsManager for the first time section in this manual

3.5 What to do next

3.5.1 Running GFI EventsManager for the first time

After installation, the GFI EventsManager console is launched automatically. To launch GFI EventsManager click **Start ► All Programs ► GFI EventsManager ► Management Console**.

Follow the steps outlined below to configure GFI EventsManager for first time use:

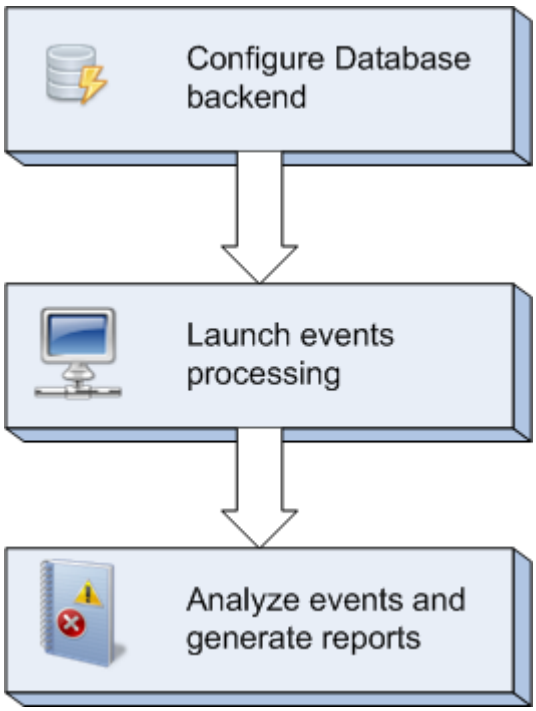
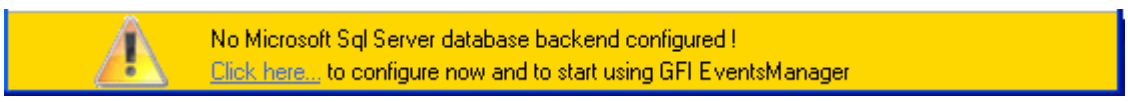


Figure 6: Running GFI EventsManager for the first time

3.5.2 Step 1: Configure the database backend

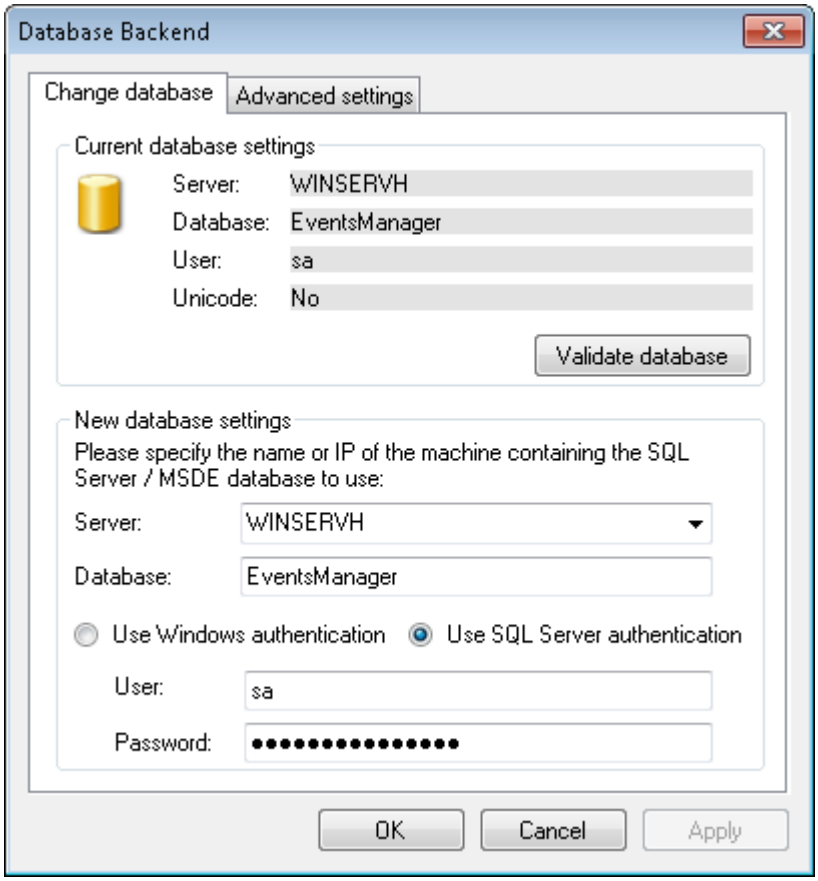
Set up the database backend on first launch of GFI EventsManager.

If you opted to install Microsoft SQL Server during the GFI EventsManager installation, the database backend required by GFI EventsManager will be set up automatically. You are therefore not required to manually create the database backend.



Screenshot 5 - Database backend alert displayed on Quick Start Dialog

An alert will appear at the bottom of the Quick Start Dialog indicating that you are required to configure a Microsoft SQL Server database backend. Select **Click here…** in the alert box to configure the Microsoft SQL backend database.



Screenshot 6 - Database Options - Change database tab

To configure the SQL Server and database backend details:

1. Specify the name/IP of your SQL Server.

2. Key in a name for your database backend (e.g. EventsManager).

3. Select the authentication method used to connect to the SQL Server. If SQL Server authentication is selected, specify the login username and password.

4. (Optional) Click **Validate database** to check that the selected database exists and has the correct structure.

5. Click **Advanced settings** tab to select the language character and symbol support to be used.

6. Click **OK** to finalize settings.

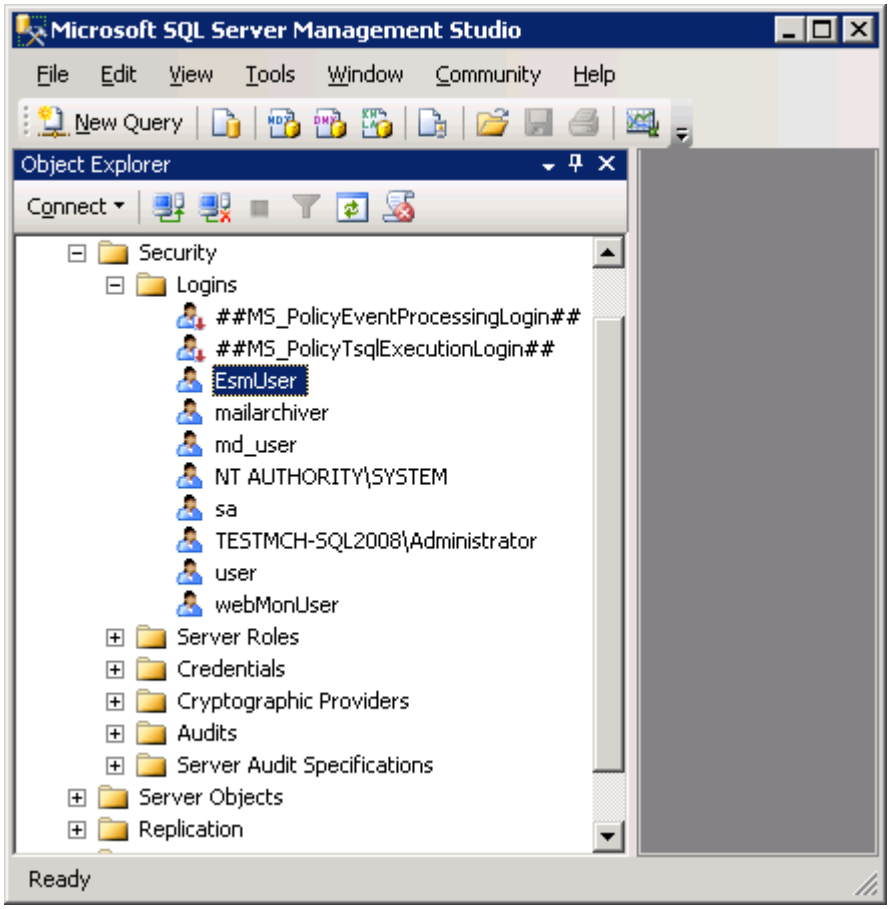
Microsoft SQL server must have TCP port 1433 open to store events collected by GFI EventsManager. For more information, refer to http://support.microsoft.com/kb/287932

The account under which GFI EventsManager is running, requires read and write access privilege on the database. To enable these privileges:

1. Launch SQL Server Management Studio and from the **Object Explorer**, expand **Security ► Logins**. Check that the account to be used by GFI EventsManager is listed in the **Logins** folder.

For Microsoft Windows Vista or later, ensure to run Microsoft SQL Server Management Studio as an Administrator.

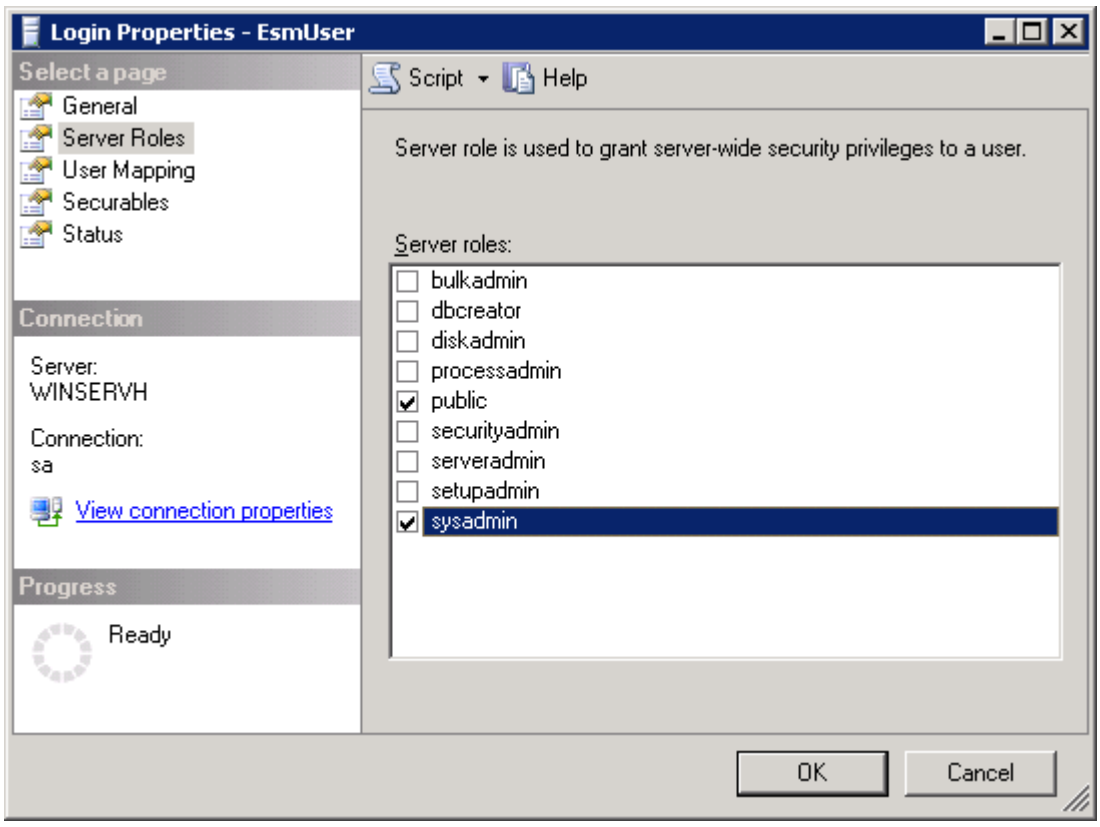
If you are using Microsoft SQL Express, download the Microsoft SQL Server Management Studio Express from: http://www.microsoft.com/downloads/details.aspx?familyid=C243A5AE-4BD1-4E3D-94B8-5A0F62BF7796&displaylang=en



Screenshot 7 - SQL Server Management - Logins folder

2. Right click the user and select **Properties**.

3. From the left panel, select **Server Roles** page and check that **sysadmin** is selected.

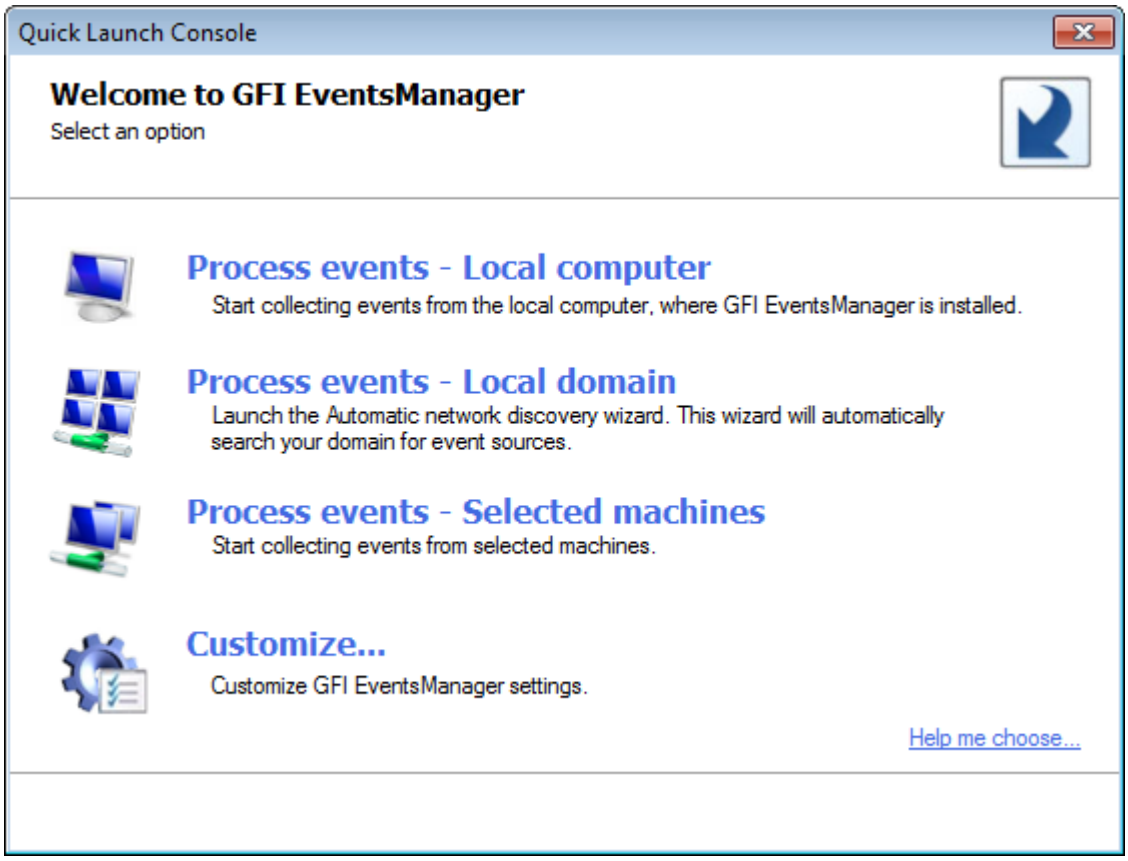


Screenshot 8 - SQL Server Management - Login Properties dialog

4. Click **OK** and close the SQL Server Management Studio.

3.5.3 Step 2: Launch events processing

You are now required to define the event sources i.e. the computers from which events will be collected.


Quick Launch Console
Welcome to GFI EventsManager
Select an option
Process events - Local computer
Start collecting events from the local computer, where GFI EventsManager is installed.
Process events - Local domain
Launch the Automatic network discovery wizard. This wizard will automatically search your domain for event sources.
Process events - Selected machines
Start collecting events from selected machines.
Customize...
Customize GFI EventsManager settings.
Help me choose...

Screenshot 9 - Quick Start Dialog

From the Quick Start dialog select one of the following options:

1. **Process events - local computer:** Start collecting events from the local computer, where GFI EventsManager is installed. For more information refer to Processing events from the local computer section in this chapter.

2. **Process events - local domain:** Launch the **Automatic network discovery** wizard. This wizard will automatically search your network for event sources. For more information refer to Processing events from the local domain section in this chapter.

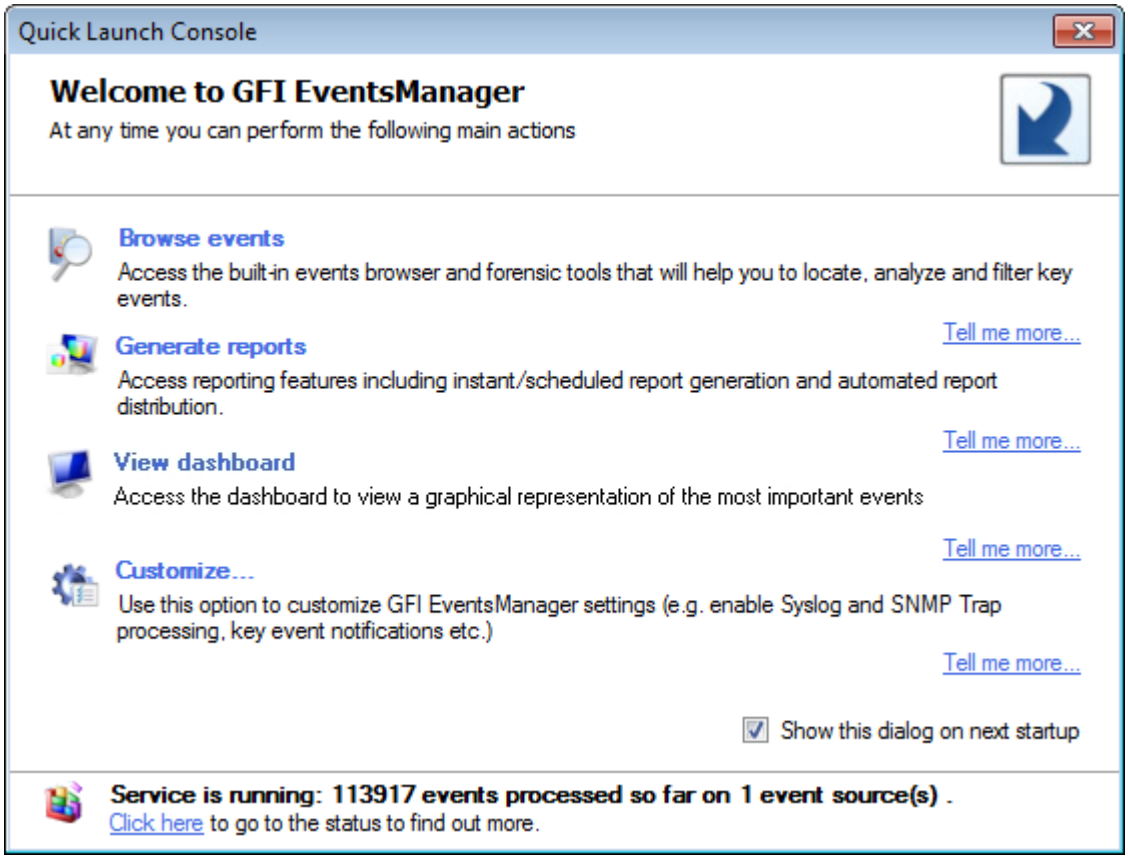
3. **Process events - selected machines:** Add event sources manually without using the wizard. For more information refer to Processing events from selected machines

4. **Customize:** Customize different types of events or different types of sources (e.g. Syslog and SNMP Trap processing).

3.5.4 Processing events from the local computer

To process event logs from the local machine:

1. From the Quick Start Dialog, click **Process events - local computer.** GFI EventsManager will start to collect events from the local machine immediately.


Quick Launch Console
Welcome to GFI EventsManager
At any time you can perform the following main actions
Browse events
Access the built-in events browser and forensic tools that will help you to locate, analyze and filter key events.
Tell me more...
Generate reports
Access reporting features including instant/scheduled report generation and automated report distribution.
Tell me more...
View dashboard
Access the dashboard to view a graphical representation of the most important events
Tell me more...
Customize...
Use this option to customize GFI EventsManager settings (e.g. enable Syslog and SNMP Trap processing, key event notifications etc.)
Tell me more...
Show this dialog on next startup
Service is running: 113917 events processed so far on 1 event source(s) .
Click here to go to the status to find out more.

Screenshot 10 - Events processed from local machine

On completion, the number of events that have been processed is displayed in the information bar as illustrated in the screenshot above.

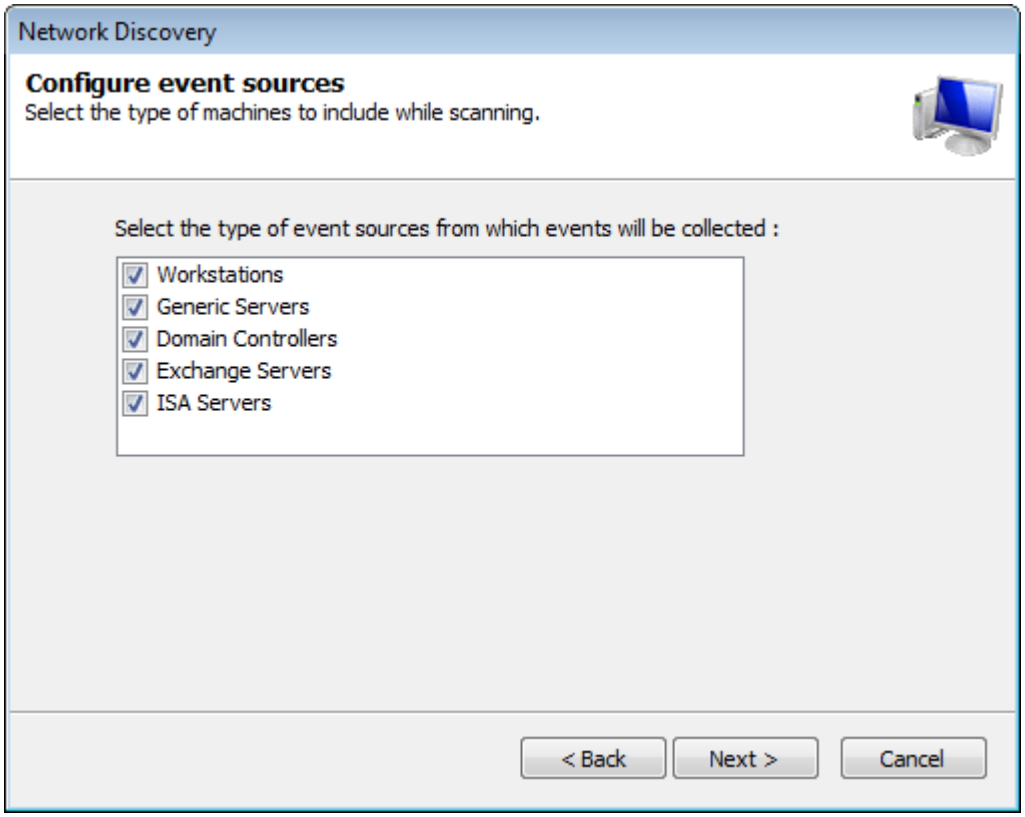
3.5.5 Processing events from the local domain

The **Network discovery wizard** searches the entire network for computers and servers. This will assist in adding network computers as GFI EventsManager event sources. To launch the Network discovery wizard:

1. From the Quick Start Dialog, click **Process events - Local domain**

	The wizard can also be launched from **Configuration ► Event Sources,** right click **All event sources** and select **Scan local domain**.
	If synchronization options are configured, **Process events - Local Domain** is disabled. For more information refer to Edit synchronization options section in this manual.

2. In the Welcome screen, click **Next**.

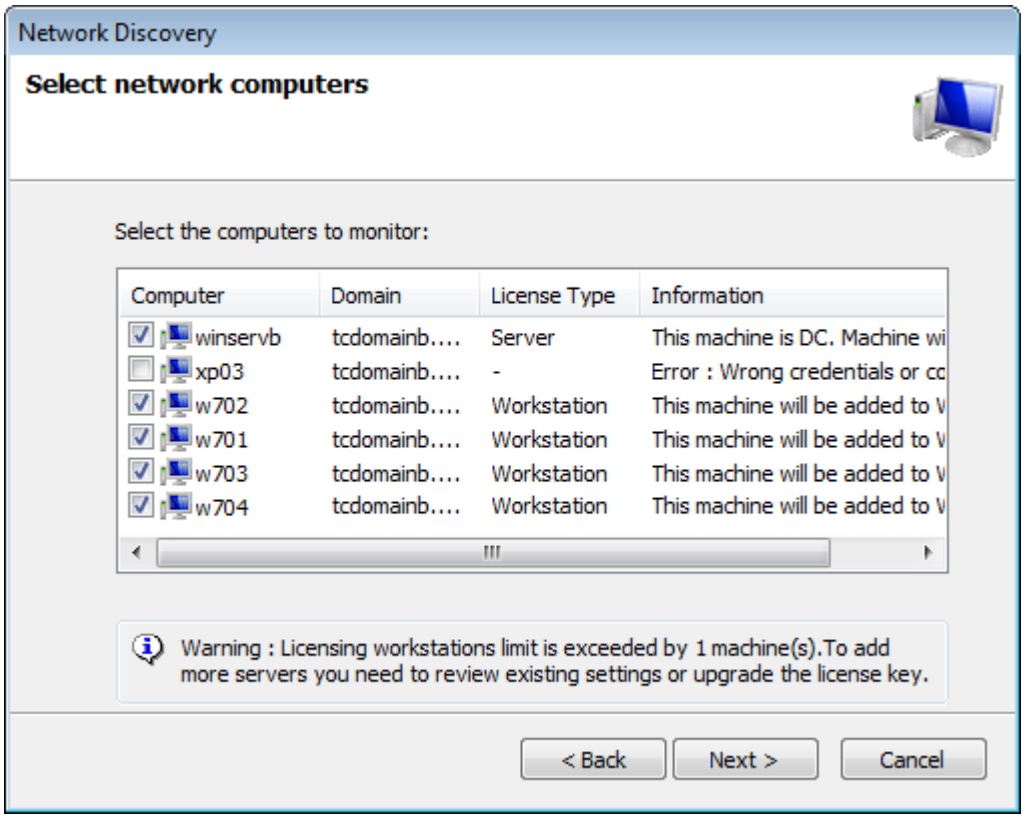


Screenshot 11 - Select the type of event source

3. The wizard enables you to search the local network for specific types of event sources. Select the type of event sources to add and click **Next**.

At least one event source type must be selected before proceeding to the next wizard dialog.

4. The wizard will automatically start to search for connected computers. On completion, click **Next**.



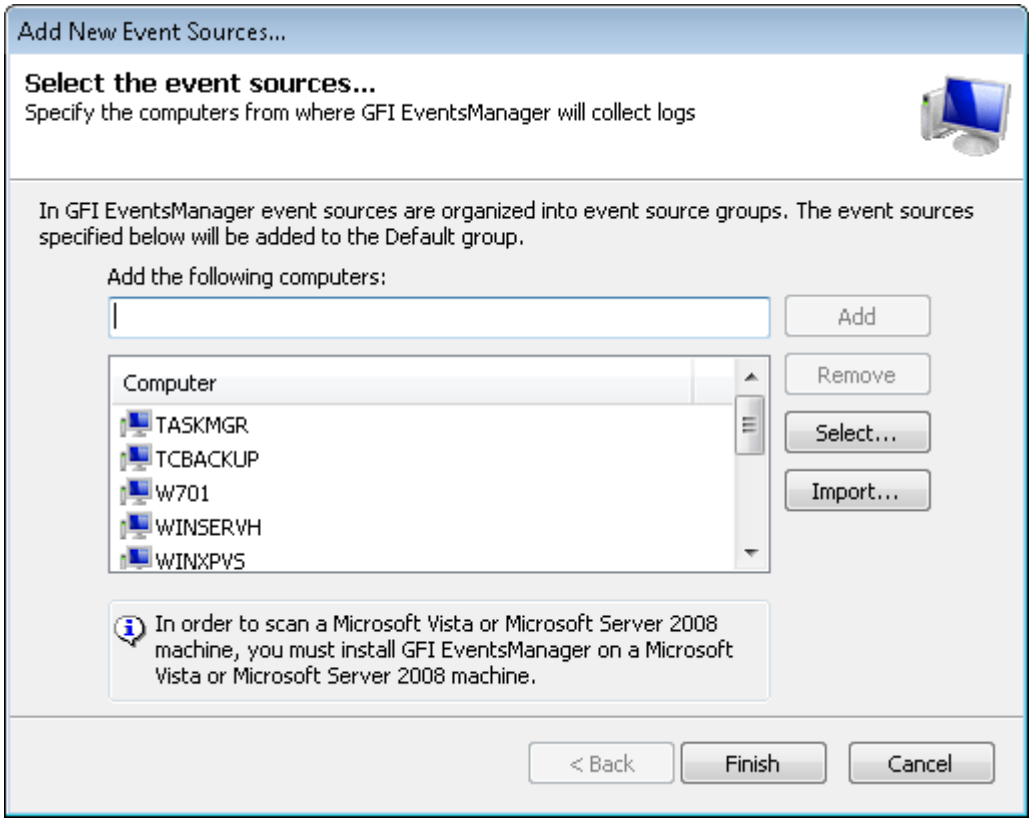
Screenshot 12 - Select computers from result

All discovered machines are by default selected. If the wizard fails to login to a target machine, it is not selected.

5. To add a machine not selected by default, click the machine and a dialog will enable you to key-in alternative credentials. Click **OK** and **Next**.

6. Click **Finish**.

3.5.6 Processing events from selected machines


Add New Event Sources...
Select the event sources...
Specify the computers from where GFI EventsManager will collect logs
In GFI EventsManager event sources are organized into event source groups. The event sources specified below will be added to the Default group.
Add the following computers:
Add
Remove
Computer
TASKMGR
TCBACKUP
W701
WINSERVH
WINXPVS
Select...
Import...
In order to scan a Microsoft Vista or Microsoft Server 2008 machine, you must install GFI EventsManager on a Microsoft Vista or Microsoft Server 2008 machine.
< Back
Finish
Cancel

Screenshot 13 - Process events from selected machines

To collect event logs from selected machines:

1. From the Quick Start Dialog, click **Process events - selected machines** to launch the **Add New Event Sources** wizard.

2. Specify the name/IP of the new event source and click **Add**. Repeat until you have specified all the event sources to add to this group.

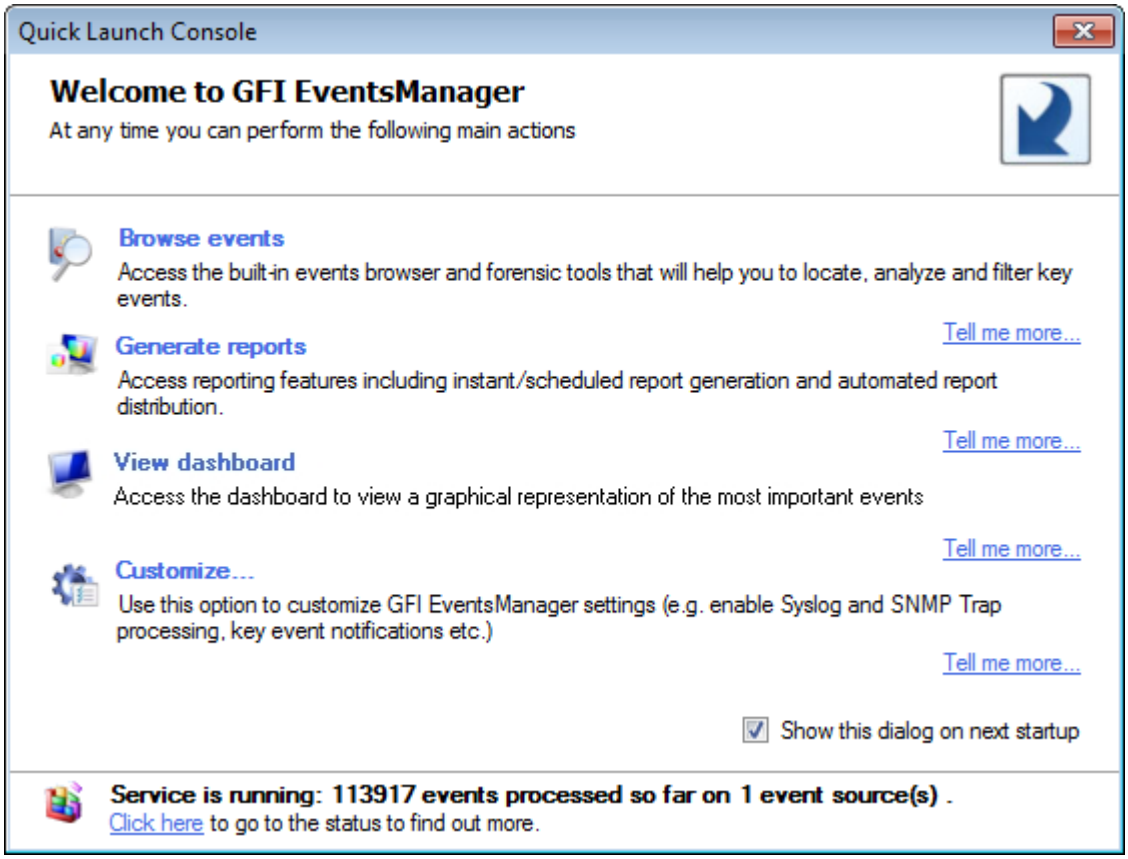
To import the list of event sources from a text file click **Import** button. To select event sources from a list, click **Select** button.

3. Click **Finish** to finalize settings. GFI EventsManager will collect events from the configured sources immediately.

3.5.7 Step 3: Analyze events and generate reports

Navigating the Quick Launch Console

You can now analyze the event information collected and generate reports based on the data gathered.


Quick Launch Console
Welcome to GFI EventsManager
At any time you can perform the following main actions
Browse events
Access the built-in events browser and forensic tools that will help you to locate, analyze and filter key events.
Tell me more...
Generate reports
Access reporting features including instant/scheduled report generation and automated report distribution.
Tell me more...
View dashboard
Access the dashboard to view a graphical representation of the most important events
Tell me more...
Customize...
Use this option to customize GFI EventsManager settings (e.g. enable Syslog and SNMP Trap processing, key event notifications etc.)
Tell me more...
Show this dialog on next startup
Service is running: 113917 events processed so far on 1 event source(s) .
Click here to go to the status to find out more.

Screenshot 14 - GFI EventsManager Quick Launch Console

Launch Console link Open Quick Start Dialog from the top right-hand corner of the GFI EventsManager user interface. Table 1 below describes the options available in the **Quick Launch Console**.

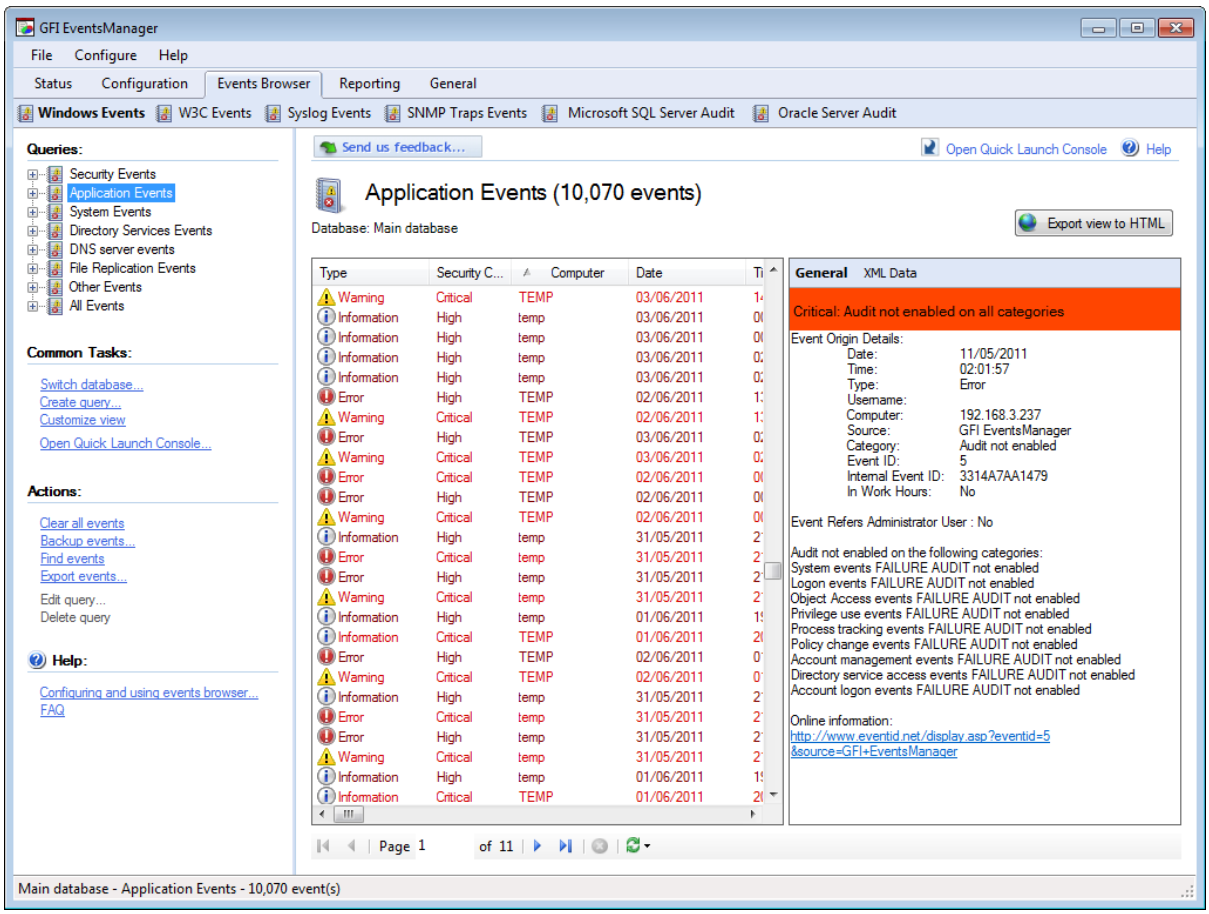
Table 1 - Quick Launch Console options

ICON	DESCRIPTION
	Browse events Access the built-in events and forensic tools that will help you to locate, analyze and filter key events. For more information refer to Event browsing chapter in this manual.
	Generate reports Access reporting features including instant/scheduled report generations and automated report distribution. For more information refer to Generating reports chapter in this manual.
	View dashboard Access GFI EventsManager status dashboard. This enables you to view graphical representations of the most important events collected and processed by GFI EventsManager. For more information, refer to Status monitoring section in this manual.
	Customize Customize GFI EventsManager settings, such as enabling Syslog, SNMP Trap processing, key events notifications, etc. For more information refer to Manage event sources chapter in this manual.

4 Event browsing

4.1 Introduction

The Event Browsing option allows you to access and browse processed or unprocessed events/logs that are currently stored in the main or backup database.

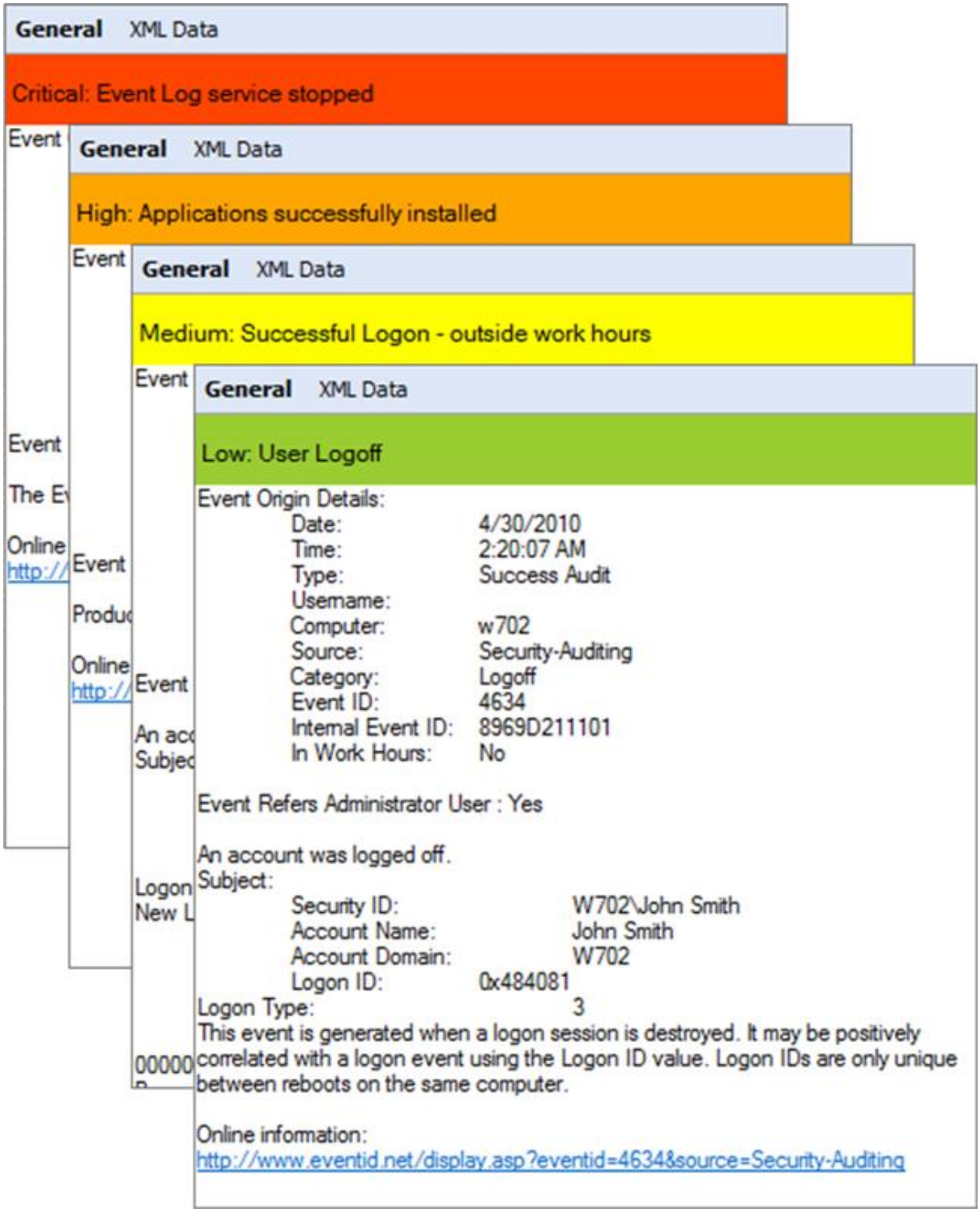


Screenshot 15 - GFI EventsManager: Events Browser

Use the **Events Browser** for forensic analysis of events. All events accessible through the **Events Browser** are organized (by log type) in the following tabs:

- Windows Events
- W3C Events
- Syslog Events
- SNMP Traps Events
- Microsoft SQL Server Audit
- Oracle Server Audit

This way you can quickly access the events belonging to a particular log type. Event data is organized into columns, click a particular event to show additional information in a dedicated events description pane. The header color coding enables you to quickly identify the severity of the event.


General XML Data
Critical: Event Log service stopped
General XML Data
High: Applications successfully installed
General XML Data
Medium: Successful Logon - outside work hours
General XML Data
Low: User Logoff
Event Origin Details:
Date: 4/30/2010
Time: 2:20:07 AM
Type: Success Audit
Username:
Computer: w702
Source: Security-Auditing
Category: Logoff
Event ID: 4634
Internal Event ID: 8969D211101
In Work Hours: No
Event Refers Administrator User : Yes
An account was logged off.
Subject:
Security ID: W702\John Smith
Account Name: John Smith
Account Domain: W702
Logon ID: 0x484081
Logon Type: 3
This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
Online information:
http://www.eventid.net/display.asp?eventid=4634&source=Security-Auditing

Screenshot 16 - Event details provided in the Events Browser

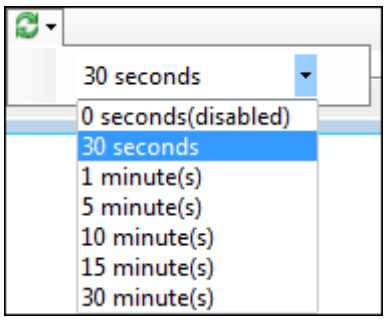
Windows events, descriptions are organized in two tabs accessible from the events description field:

- **General tab -** Contains events information in the legacy format that was standard for pre-Microsoft Windows Vista event logs.
- **XML Data tab -** Contains events information in the new XML based Microsoft Windows Vista format.

Use the link provided in the event description pane to access:

- A more detailed description of the event
- Information and links that explain what causes this type of event
- Hints and tips on how to possibly solve any existing issues.

The navigation tool bar allows you to navigate between pages, stop a query and configure the auto-refresh rate. To configure auto-refresh, click the refresh icon and select the required time interval.



Screenshot 17 - Configure auto-refresh

Event analysis is quite a demanding task; GFI EventsManager is equipped with specialized tools that simplify the search for specific events as well as enable the export of events to CSV and HTML files. These specialized tools include:

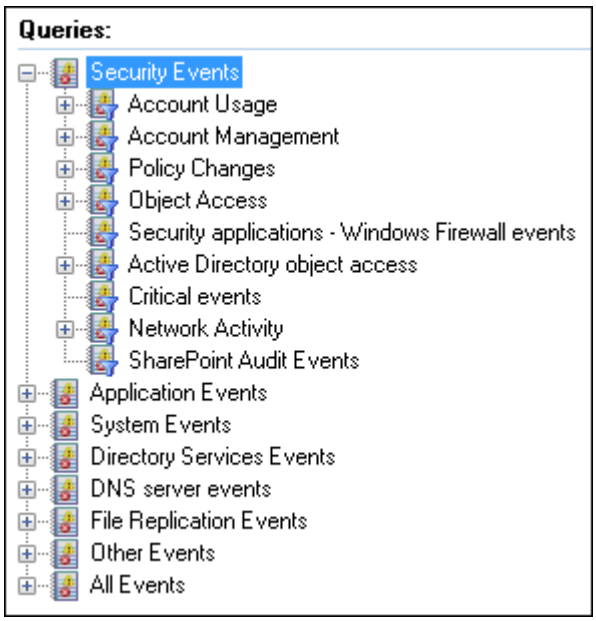
- An event filter/query builder
- Event color-coding options
- Event finder tool
- Export events tool
- Rule finder tool.

4.2 Event filter/query builder

Use the event query builder to create custom filters that sift events data and display only the information needed. To filter event during browsing:

1. Click **Events Browser** tab and select the event browser required.

2. From the left pane select the required events filter (such as the Accounts Usage filter). Results will be displayed in the browser (right pane).



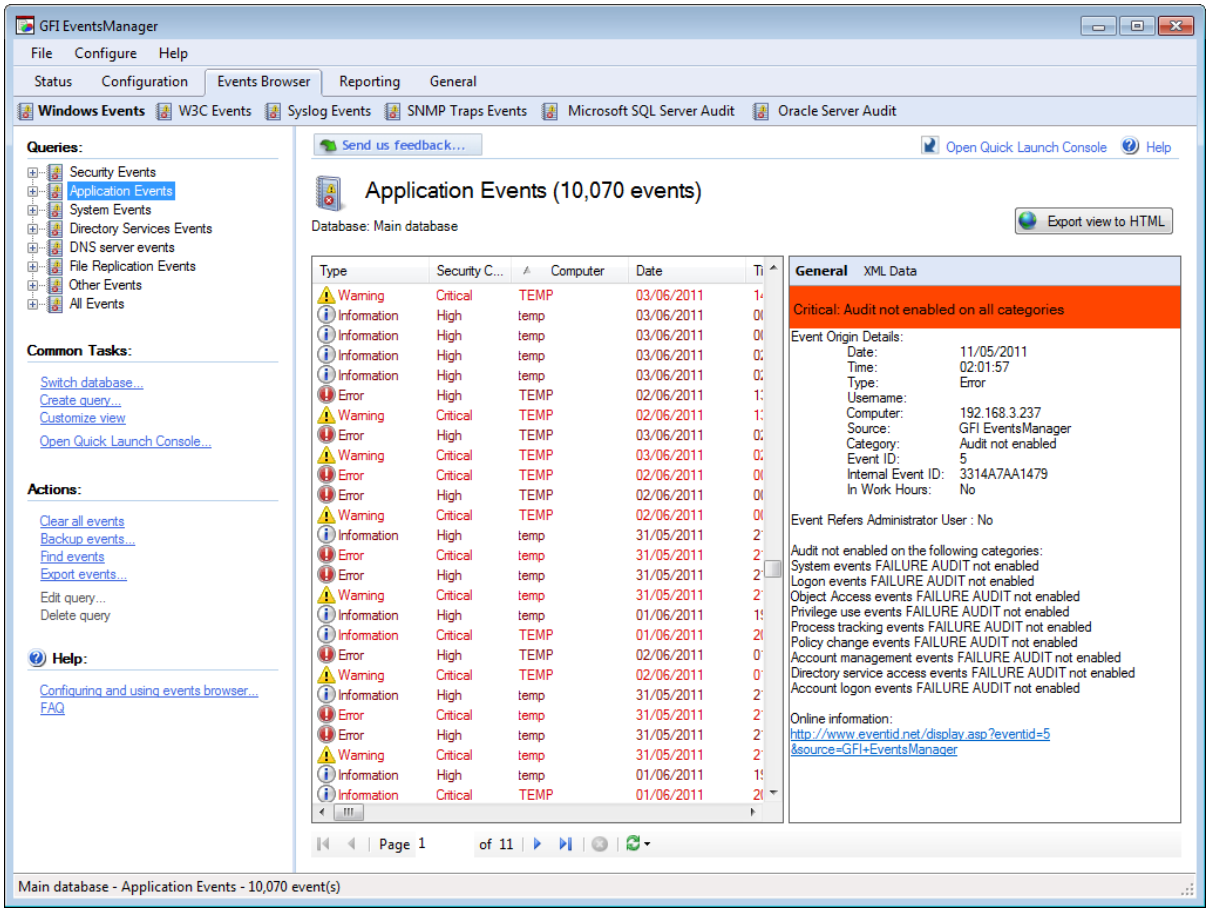
Screenshot 18 - Selecting a filter

4.2.1 Creating custom event queries

In GFI EventsManager, custom queries are added as a sub-node within the default queries that ship with the product. To create custom event queries:

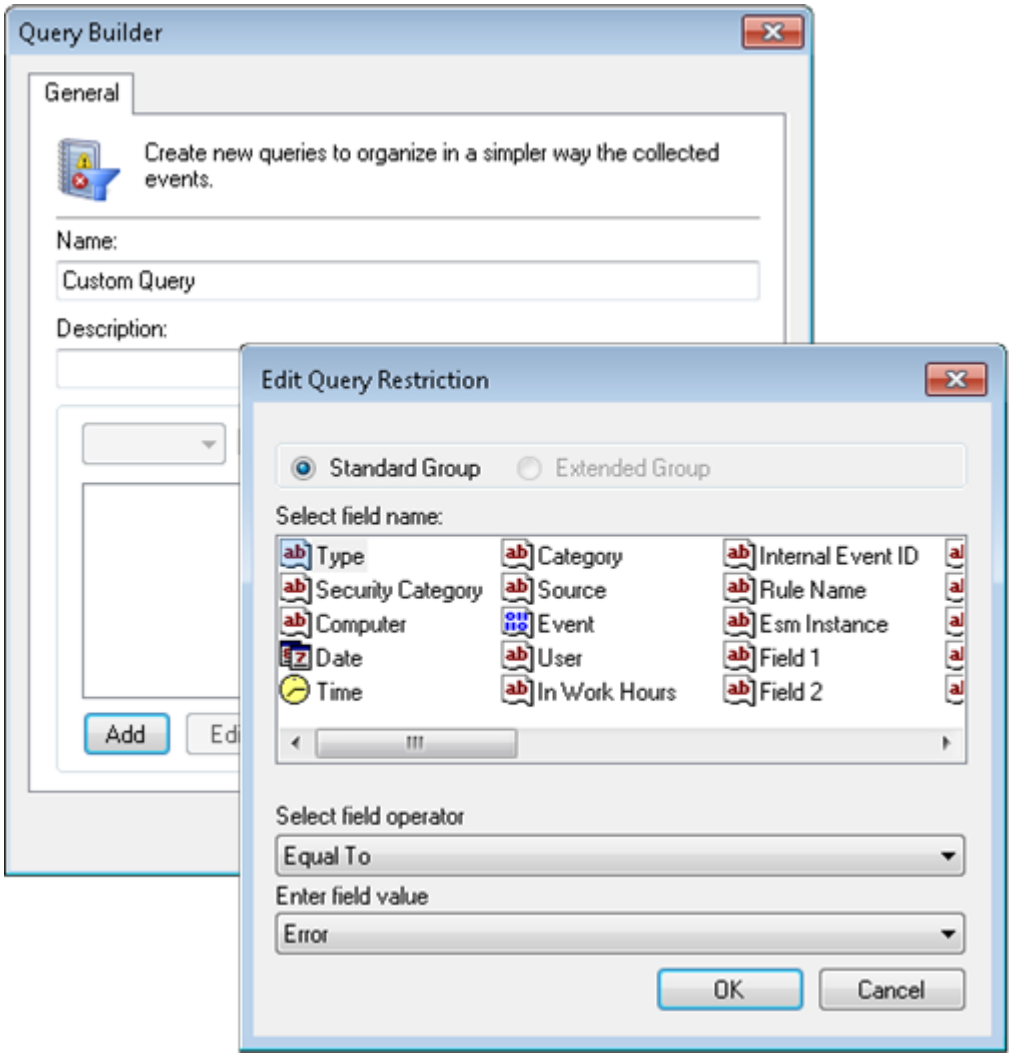
1. Click **Events Browser** tab and select one of the following tabs:

- Windows Events
- W3C Events
- Syslog Events
- SNMP Traps Events
- Microsoft SQL Server Audit
- Oracle Server Audit



Screenshot 19 - GFI EventsManager: Events Browser

2. Right-click default query where the new event query will be created and select **Create query…**



Screenshot 20- Custom query builder

3. Specify a name and a description for the new query.

4. Click **Add**, configure the required query condition(s) and click **OK**. Repeat until all required query conditions have been specified. For more information on field operators refer to Field operator section in this manual.

5. Click **OK** to finalize your settings.

4.2.2 Create query from an existing event

GFI EventsManager allows the administrator to sort events automatically by creating custom queries. Each query has its own filtering criteria, and administrators can create a query by selecting a particular field from an existing event. The selected field will automatically be included in the filtering criteria. To automatically create a query based on a field:

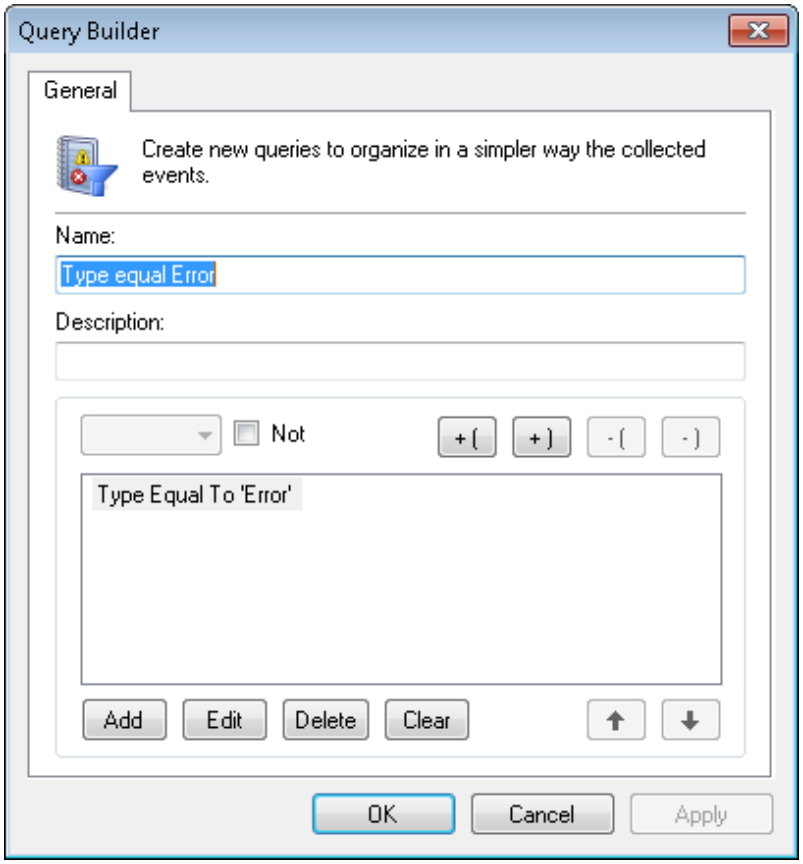
1. Click **Events Browser** tab.

2. From the **Queries** list, select the type of query and the existing event.

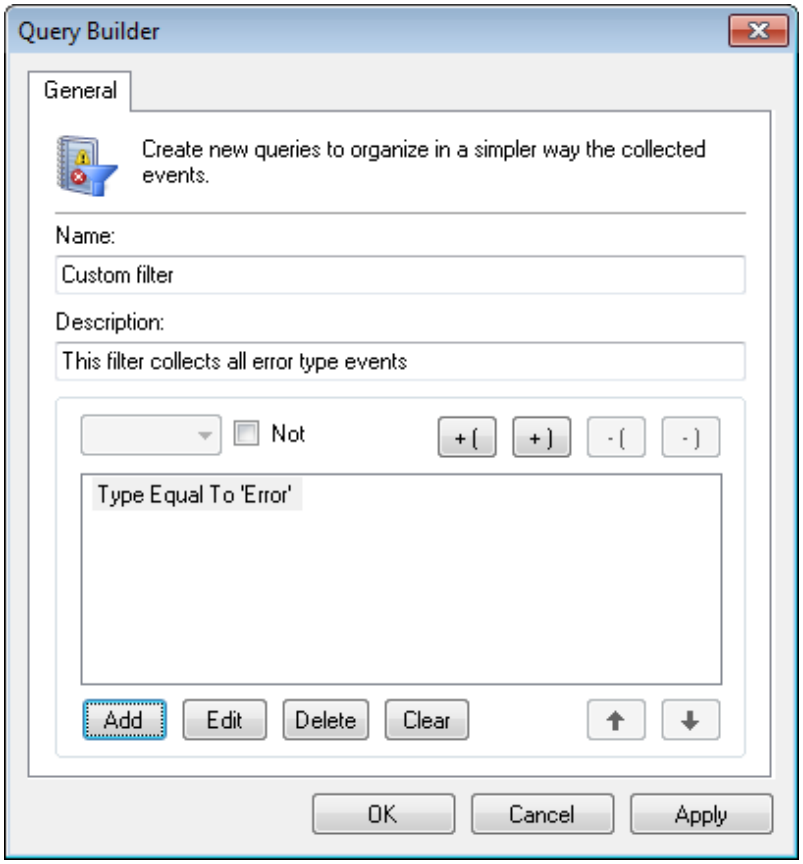
3. Right click the field that will be included in the query builder, and click **Create query from field**.

4.2.3 View or Edit a custom query

The naming convention of the new query is **Type equal <Field Selected>**. To edit the query, right click the query and select **Properties**.

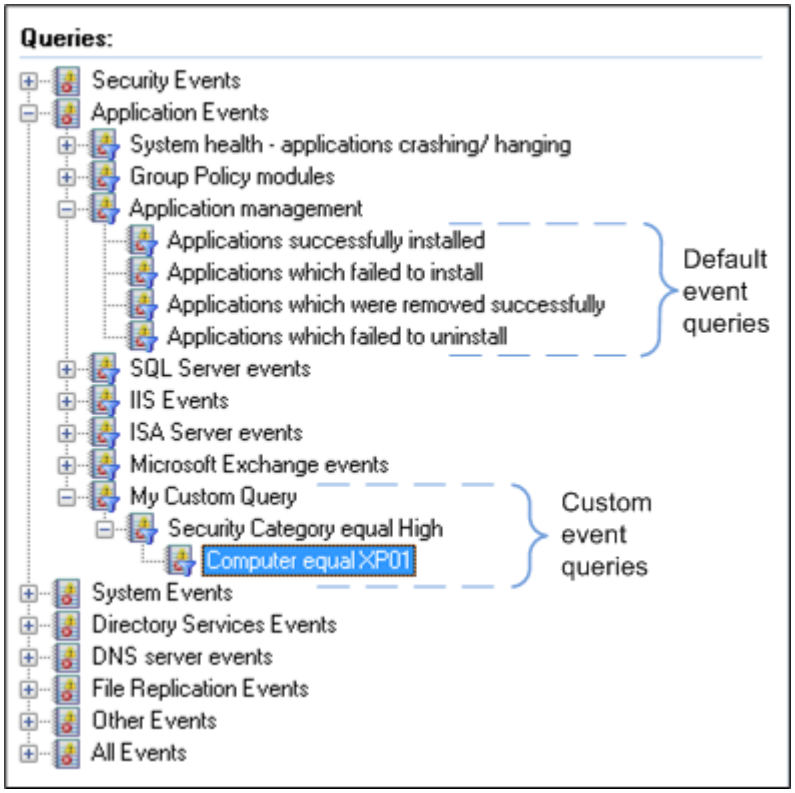


Screenshot 21 - Query builder for an existing query



Screenshot 22 - Create new query using the query builder

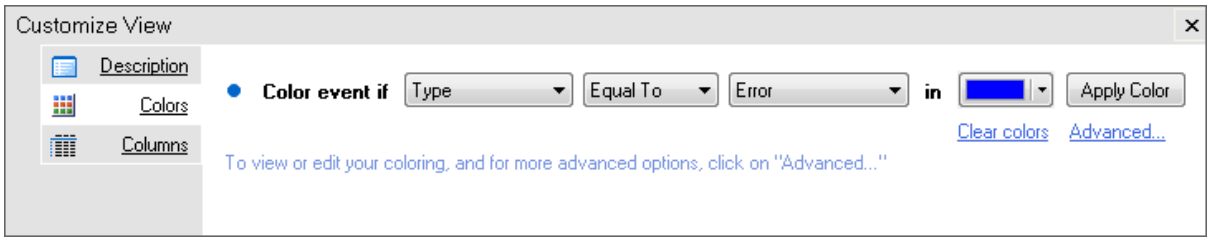
GFI EventsManager ships with pre-configured queries that can filter events without any configuration effort.



Screenshot 23 - Default and custom event queries

4.3 Event color-coding options

Use the event color-coding tool to tint key events in a particular color. This way the required events are easier to locate during event browsing. For example, you can create a query that shows events classified as Critical or High and at the same time color in red all Critical events having event ID 231.

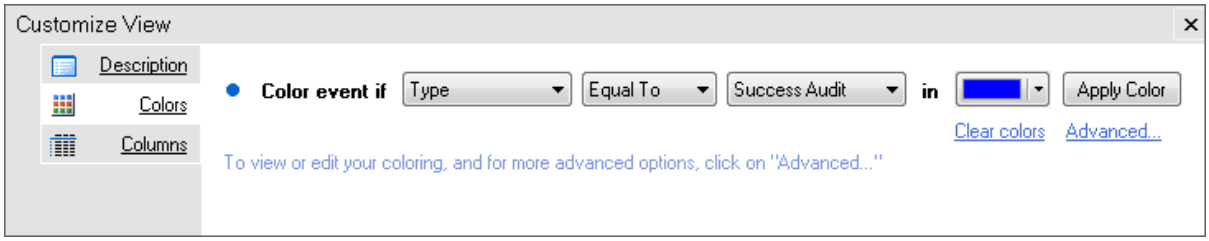


Screenshot 24 - Color coding configuration

The configuration of color-codes is carried out through a dedicated query builder. To use the query builder click **Advanced** and configure the following options:

- The conditions that define which events must be colored
- The colors to be used when showing these events.

4.3.1 Assigning a color-code to a specific event



Screenshot 25 - Assigning event color-codes

To assign a color code to a specific event:

1. Click **Events Browser** tab and select an events browser accordingly.

2. Select the **Customize view** option and from the right pane, select the **Colors** option.

3. Specify event filter parameters including the color to be applied to the sifted events.

4. Click **Apply Color** button to finalize your settings.

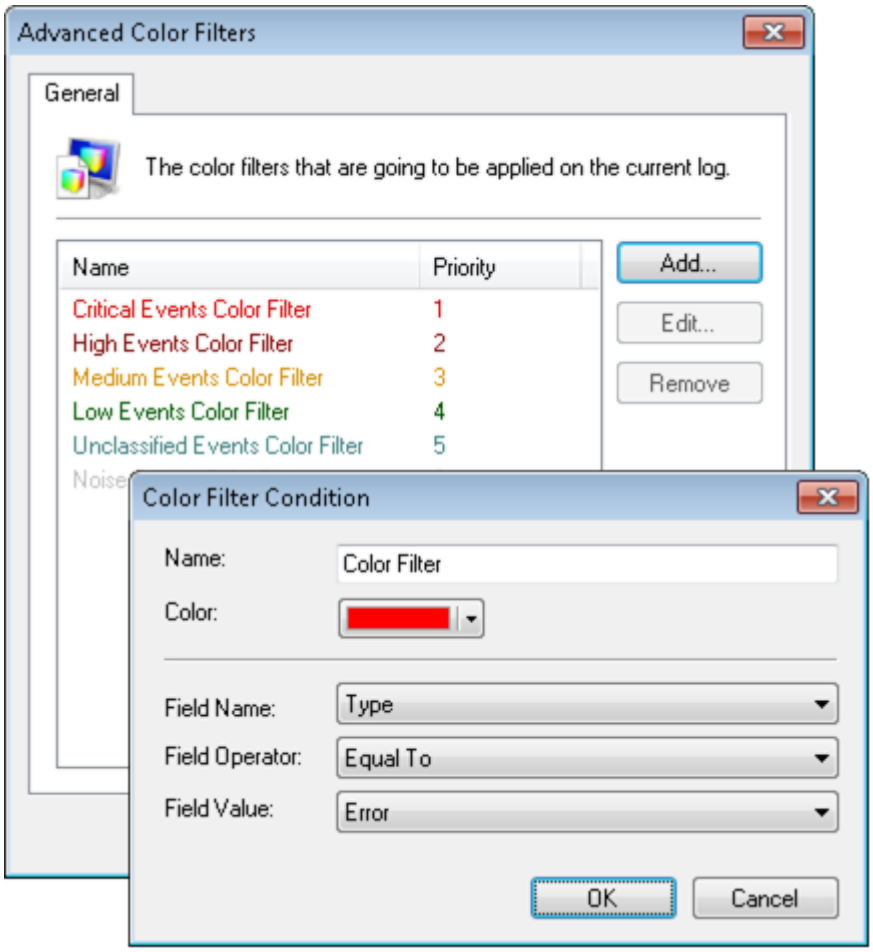
Use the **Clear color filters** option to clear all color settings.

4.3.2 Assigning different color-codes to multiple events

To assign different color-codes to multiple events:

1. Click **Events Browser** tab and select an events browser accordingly.

2. Select the **Customize view** option. From the right pane, select the **Colors** option and click **Advanced**.



Screenshot 26 - Advanced Color Filter

3. Click **Add** button. Specify filter name and configure event filter parameters.

4. Click **OK** button to save filter settings.

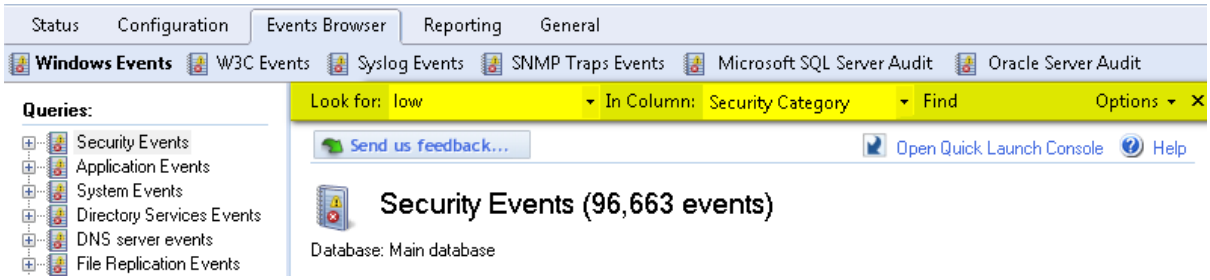
5. Repeat until all required event filter conditions have been configured. Click **OK** to finalize your settings.

4.4 Event finder tool

Use the event finder tool to locate events that match a specific search string. For example, you can search events that have a specific ID or which contain specific keywords in the description. Use the event finder tool to search and locate specific events using simple customizable filters. To search for a particular event:

1. Click **Events Browser** tab and select an events browser accordingly

2. From the left pane, select the **Find events** option.



Screenshot 27 - Event finder tool

3. Configure the event search parameters through the options provided on top of the right pane. To trigger a case sensitive search, click on **Options** and select the **Match case** option.

4. Click **Find** button to trigger the search.

4.5 Export events tool

To access and browse events stored in the database backend, click **Events Browser** tab and select a browser accordingly.

4.5.1 Export To CSV tool

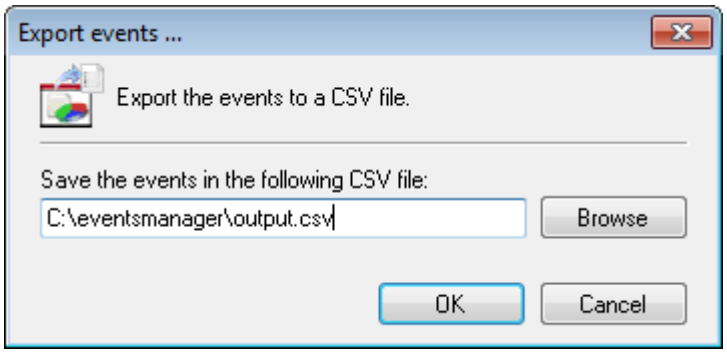
GFI EventsManager enables you to export event data to CSV files directly from the built-in event-browsers. This is extremely convenient especially when further processing of event data is required. This includes:

- Distribution of key event data via email
- Running automated scripts that convert CSV exported events data to HTML for upload on web/company intranet
- Generation of graphical management reports and statistical data using native tools such as Microsoft Excel
- Generation of custom reports using third party applications.
- Interfacing events data with applications and scripts built in-house

To export events to CSV:

1. Click **Events Browser** tab and select the required event browser.

2. Select the events to export. Right click selection and choose **Export events…**.



Screenshot 28 - Export events tool

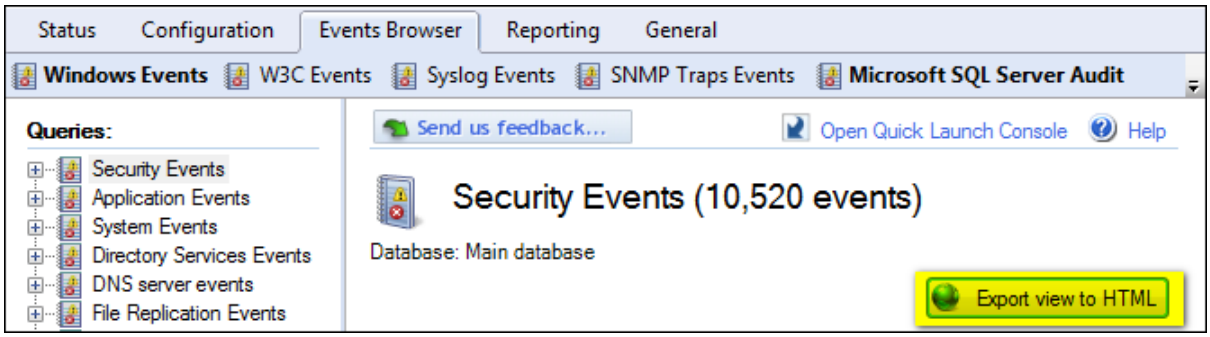
3. Specify where exported events will be saved and click **OK** to trigger the export.

4.5.2 Export to HTML tool

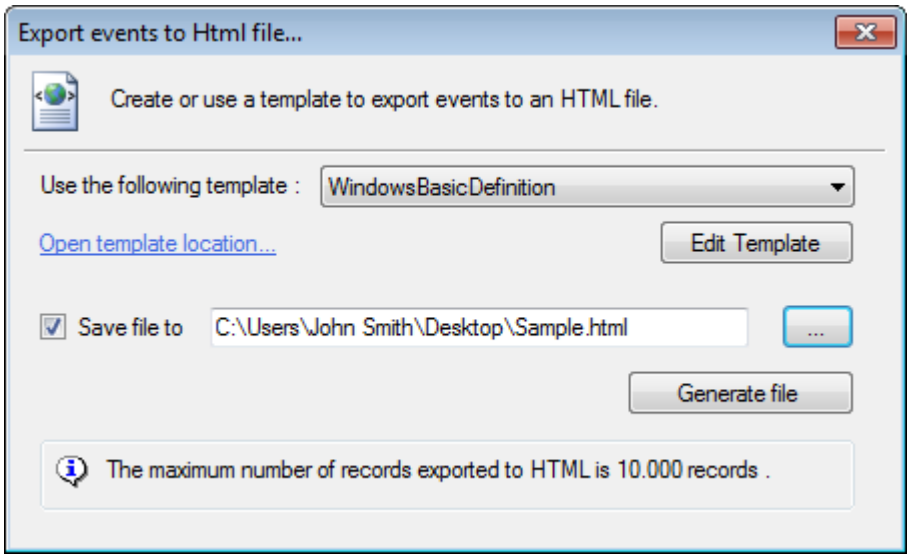
GFI EventsManager enables users to export events to HTML files. Use this feature to generate custom reports. Users have the possibility to add, rename or remove column headings and edit field parameters to choose specific data to display.

To export events to HTML:

1. Go to **Events Browser** and click **Export view to HTML**.



Screenshot 29 - Export to HTML


Export events to Html file...
Create or use a template to export events to an HTML file.
Use the following template :
WindowsBasicDefinition
Open template location...
Edit Template
Save file to
C:\Users\John Smith\Desktop\Sample.html
...
Generate file
The maximum number of records exported to HTML is 10.000 records .

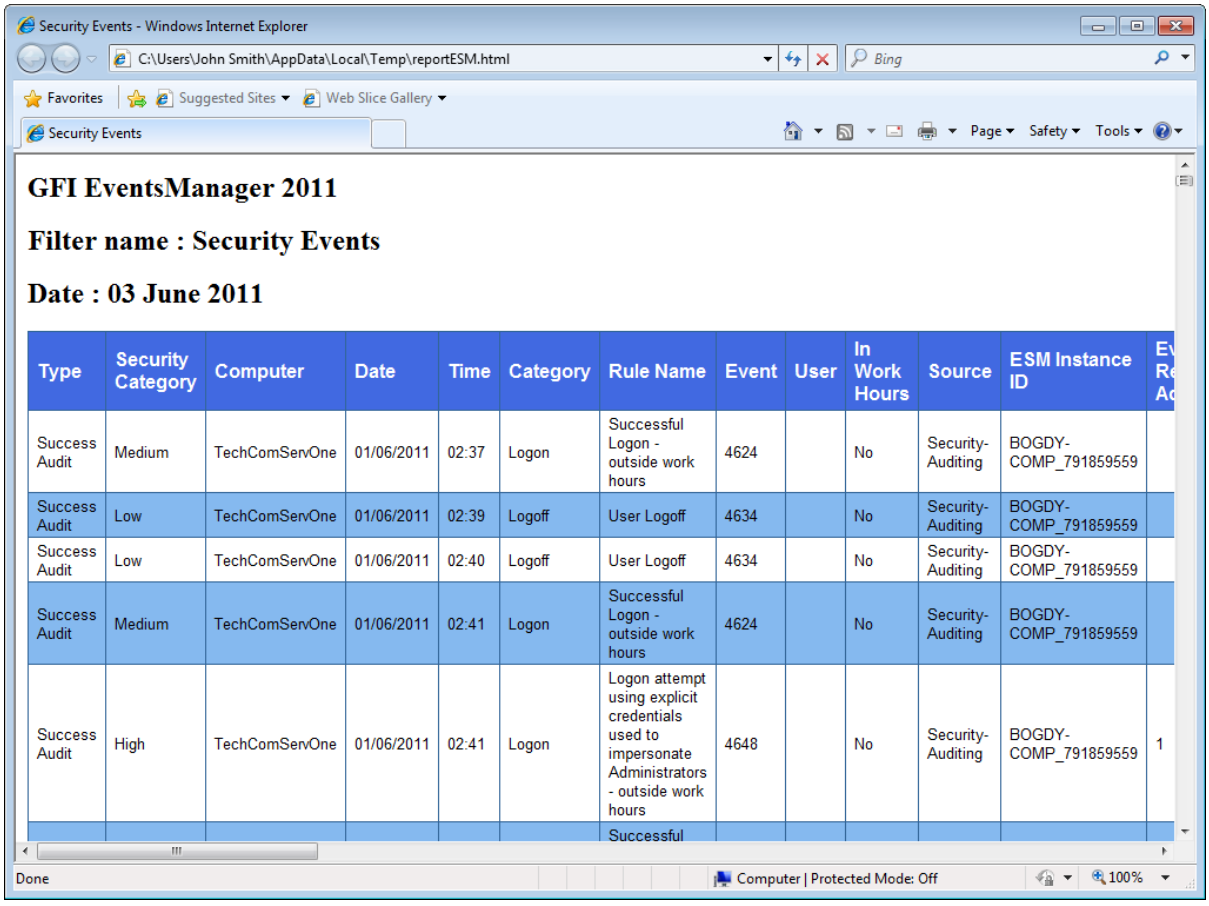
Screenshot 30 - Export to HTML dialog box

2. Configuration options are described in

Table 2 below:

Table 2 - Export to HTML options

OPTION	DESCRIPTION
Use the following template:	Uses the selected template from the drop-down menu.
Edit Template	Launches the template editor for the selected template. For more information on how to add / edit templates refer to the Adding and Editing Templates section in this manual.
Open template location	Opens the location where the templates are stored.
Save file to	Specify a location where the report is saved. Alternatively, press the '…' (Browse) button to select a location.
Generate file	Starts the output process and saves the HTML file.



Type	Security Category	Computer	Date	Time	Category	Rule Name	Event	User	In Work Hours	Source	ESM Instance ID	Ev Re Ac
Success Audit	Medium	TechComServOne	01/06/2011	02:37	Logon	Successful Logon - outside work hours	4624		No	Security-Auditing	BOGDY-COMP_791859559	
Success Audit	Low	TechComServOne	01/06/2011	02:39	Logoff	User Logoff	4634		No	Security-Auditing	BOGDY-COMP_791859559	
Success Audit	Low	TechComServOne	01/06/2011	02:40	Logoff	User Logoff	4634		No	Security-Auditing	BOGDY-COMP_791859559	
Success Audit	Medium	TechComServOne	01/06/2011	02:41	Logon	Successful Logon - outside work hours	4624		No	Security-Auditing	BOGDY-COMP_791859559	
Success Audit	High	TechComServOne	01/06/2011	02:41	Logon	Logon attempt using explicit credentials used to impersonate Administrators - outside work hours	4648		No	Security-Auditing	BOGDY-COMP_791859559	1
						Successful						

Screenshot 31 - HTML Report Sample

4.5.3 Adding and Editing Templates

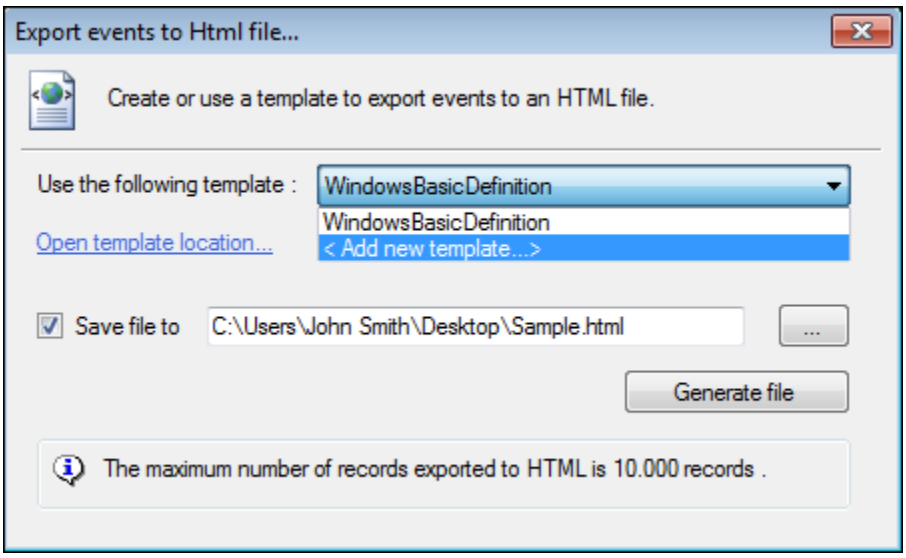
The export to HTML feature enables users to:

» Add new templates

» Edit predefined templates by adding, renaming or removing column headings. Also add or edit field parameters to choose what data the report returns.

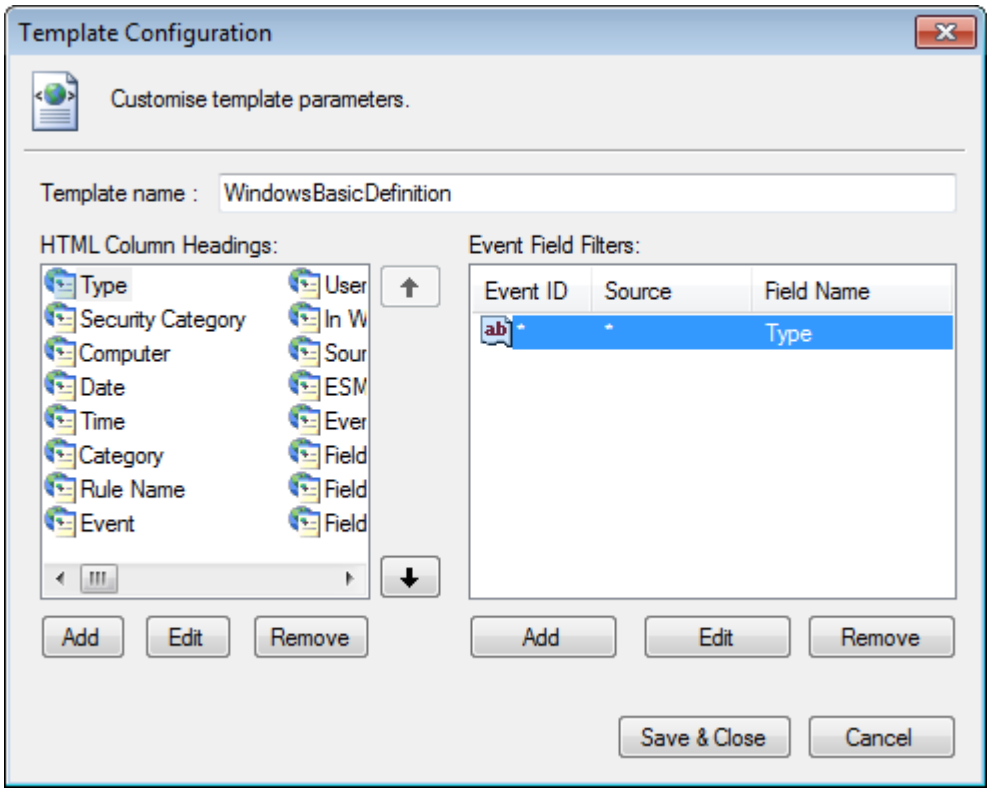
To add / edit templates:

1. From **Events Browser** click **Export view to HTML**.


Export events to Html file...
Create or use a template to export events to an HTML file.
Use the following template :
WindowsBasicDefinition
WindowsBasicDefinition
< Add new template...>
Open template location...
Save file to
C:\Users\John Smith\Desktop\Sample.html
...
Generate file
The maximum number of records exported to HTML is 10.000 records .

Screenshot 32 - Add new template

2. Select **<Add new template…>** from **Use the following template:** drop-down menu.



Screenshot 33 - Define Template

3. Use the **Define Template** dialog to add templates or edit template parameters. Configuration options are described in Table 3 below:

Table 3 - Add/Edit Template Options

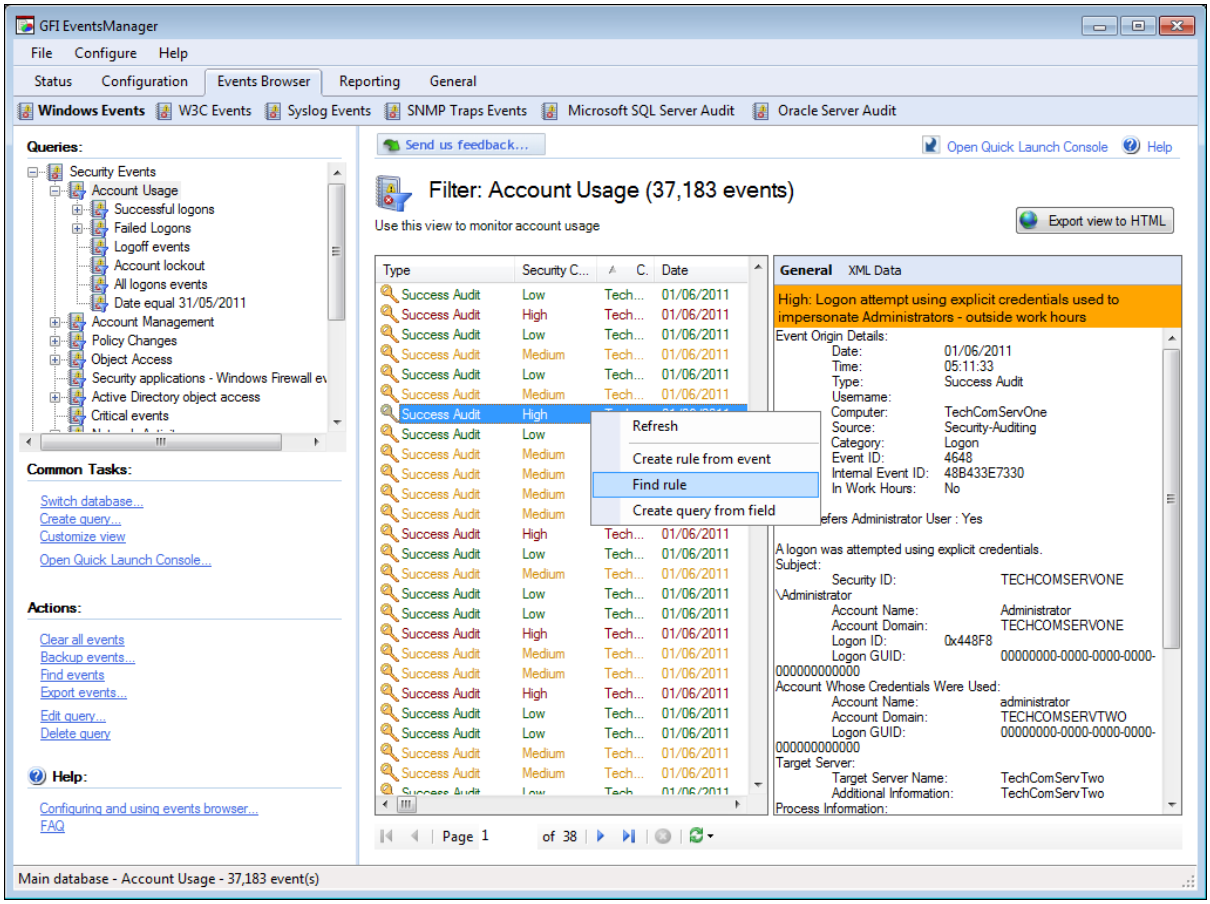
OPTION	DESCRIPTION
Template name	Specify the name of the new template.
Column name	The list of column headings included in the report.
Add (Column Name)	Click **Add** to include additional columns to the report.
Edit (Column Name)	Click **Edit** to modify column heading names.
Remove (Column Name)	Click **Remove** to remove a column from the report.
Event Fields	This section enables you to add or edit field parameters such as Event ID and Event Source.
Add (Event Fields)	Click **Add** to add new fields.
Edit (Event Fields)	Click **Edit** to edit the parameters of the selected field.
Remove (Event Fields)	Click **Remove** to remove the selected field.
Save & Close	Saves the changes applied to the new or edited template and closes the template editor.

4.6 Rule finder tool

GFI EventsManager enables you to find event processing rules from event logs in Events Browser.

To identify the rule(s) used for a specific event:

1. From **Events Browser**, right-click an event log.



Screenshot 34 - Find rule

2. Click **Find rule.**

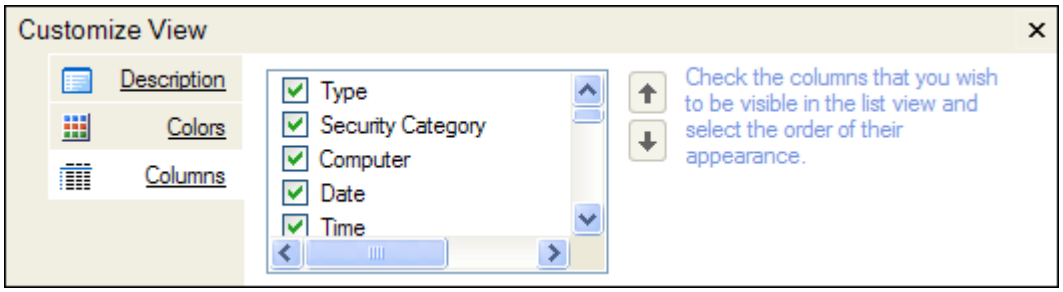
4.7 Customizing the event viewer pane

Select columns to be displayed

To select which columns will be displayed in the Log Browser's viewing pane:

1. Click **Events Browser** tab and select an events browser accordingly.

2. Select the **Customize view** option from the 'Common Tasks' area in the left pane.



Screenshot 35 - Customize view: columns

3. Select the **Columns** option.

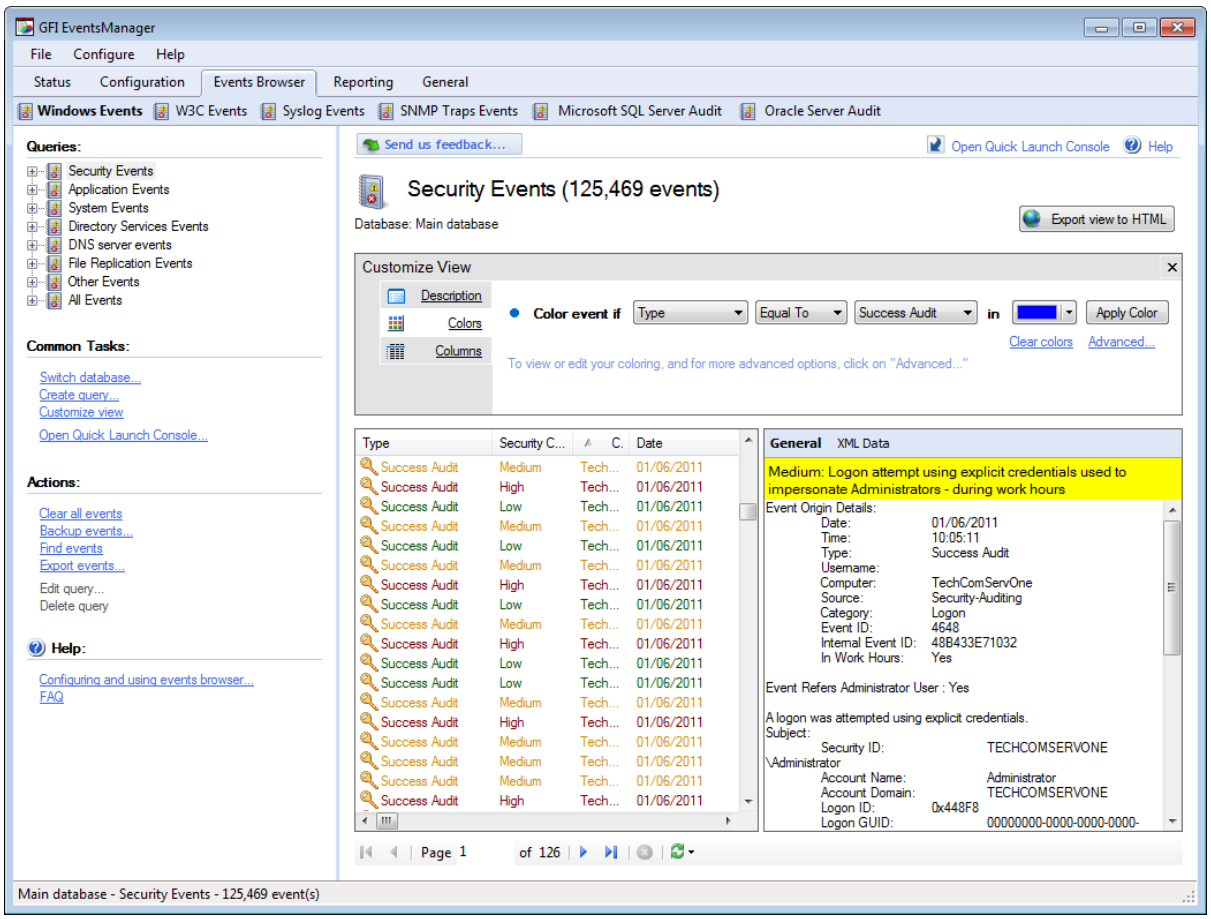
4. Select the columns that will be displayed in the viewing pane. Use the up/down arrows on the side to define the order in which the columns will be shown.

5. Close the customize view pane to finalize your settings.

Customize the position of the description window

GFI EventsManager allows you to customize the right viewing pane. To achieve this:

1. Click **Events Browser** tab and select an events browser accordingly.



Screenshot 36 - Customize view

2. Click the **Customize view** option from the **Common Tasks** pane.

3. Customize the browser view accordingly.

4.8 Event maintenance

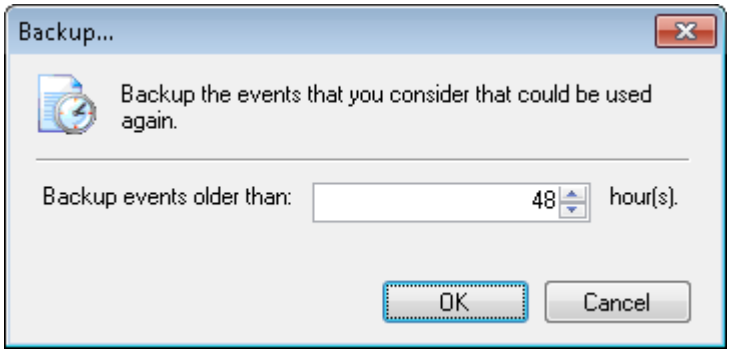
4.8.1 Backup events

GFI EventsManager allows you to backup the events stored in the main database backend. This way you can reduce the size of your main database backend but at the same time keep all your event records for historical and forensic investigation purposes.

Use the backup events feature to backup events that are older than a specific amount of hours. For example, you can choose to backup events that are older than 48 hours. To backup events:

1. Click **Events Browser** tab and select an events browser accordingly.

2. From **Actions**, select the **Backup events**.



Screenshot 37 - Backup events dialog box

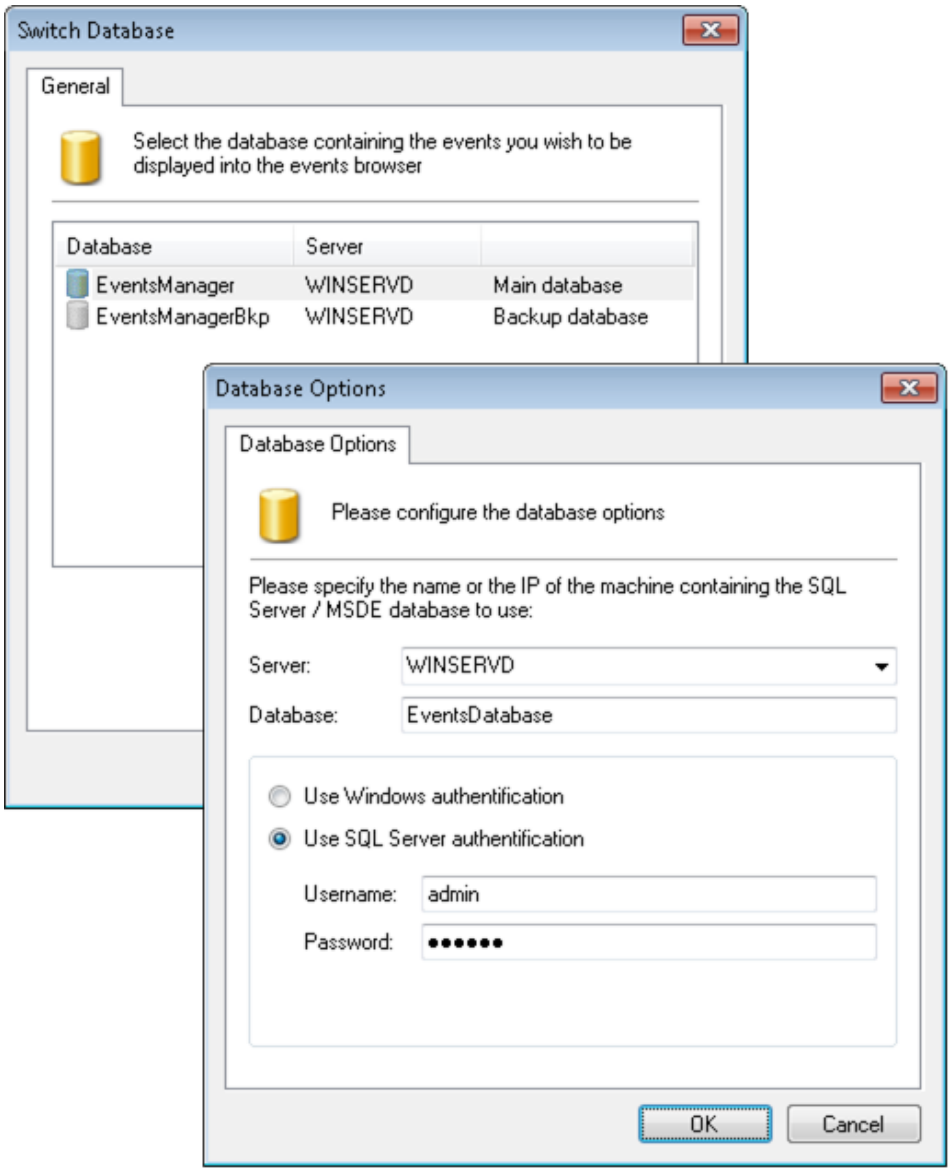
3. Specify backup parameters and click **OK** button to finalize your settings.

4.8.2 Switching databases

For event browsing purposes, GFI EventsManager allows you to switch between different databases. Use this feature to browse events that have been backed up, using the tools provided in the Events Browser. To achieve this:

1. Click **Events Browser** tab and select an events browser accordingly.

2. From the **Common Tasks**, select the **Switch database**.



Screenshot 38 - Add a new database from the switch database dialog

3. Double click the destination database (were the events will be stored), or click **Add** to create a new database.

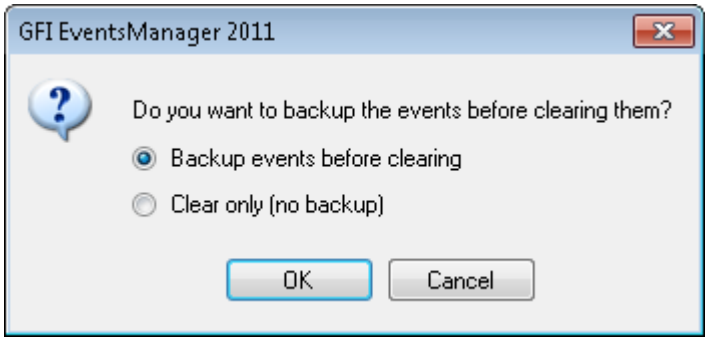
4.8.3 Clear events from a query result

To clear a group of events from the currently selected database:

1. Click **Events Browser** tab and select an event browser accordingly.

2. From **Queries**, select the query that will be cleared.

3. From **Actions**, select **Clear all events**.



Screenshot 39 - Clear all events dialog box

4. Select between:

» Backup events before clearing - Selected events will be stored in the backup database.

» Clear only (no backup) - Selected events will be removed from the Event Browser and deleted from the database.

5. Click **OK**.

To clear all events from the database, create a new database operation to delete the data. For more information on how to create a delete operation, refer to Delete data section in this manual.

5 Generating reports

5.1 Introduction

GFI EventsManager provides you with a free, fully-fledged reporting companion to GFI EventsManager - GFI EventsManager ReportPack. It enables you to generate graphical IT-level, technical and management reports based on the hardware and software events processed by GFI EventsManager. Hardware and software event sources include any networked component that generate Syslog messages or record/log events to Windows and/or W3C event logs. These include computers, network devices, PABXs, and third party software solutions.

To access GFI EventsManager ReportPack, click the **Reporting** tab.

To generate reports, the following add-ons must be downloaded and installed:

» GFI ReportCenter framework

» GFI EventsManager ReportPack

More information on how to download the GFI EventsManager ReportPack and the GFI ReportCenter framework is provided in the Download the GFI EventsManager ReportPack section in this chapter.

5.2 Daily Digest

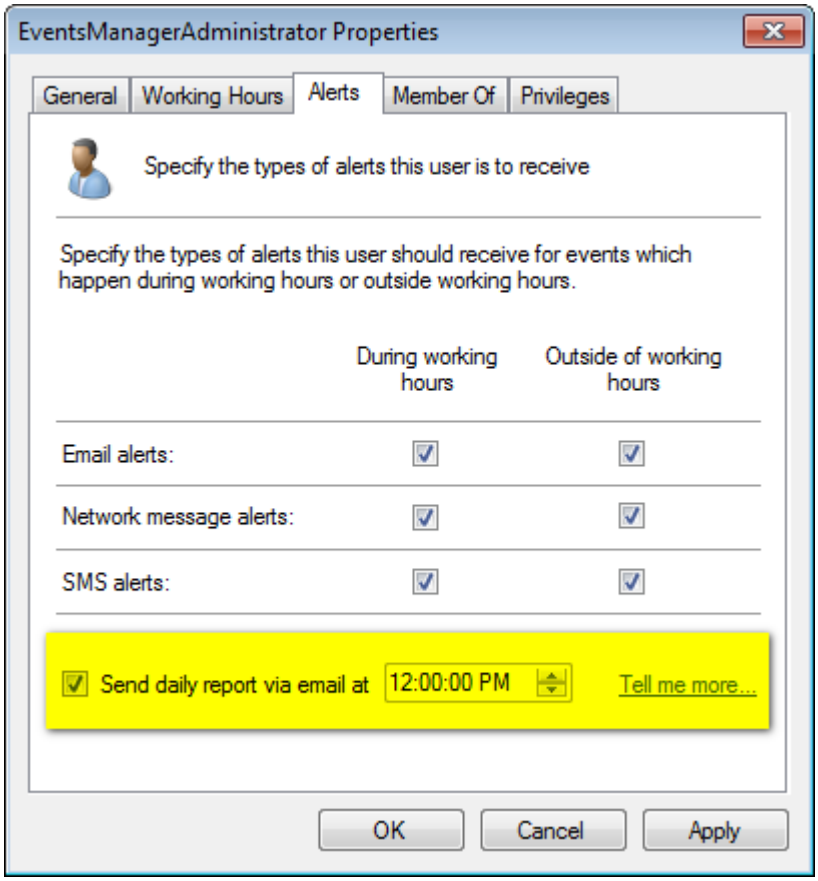
GFI EventsManager can be configured to send a summary report by email on a daily basis. The report contains a summary of the most important events collected and processed during the last 24 hours. To configure a user to receive Daily Digest emails:

1. Launch GFI EventsManager and select **Configuration** tab ► **Options**. Expand **Users and Groups** and select **Users**.

2. Right click a user from the right pane and select **Properties**.

3. Select **General** tab and ensure that a valid email address is configured.

4. Open **Alerts** tab and select **Send daily report via email**.

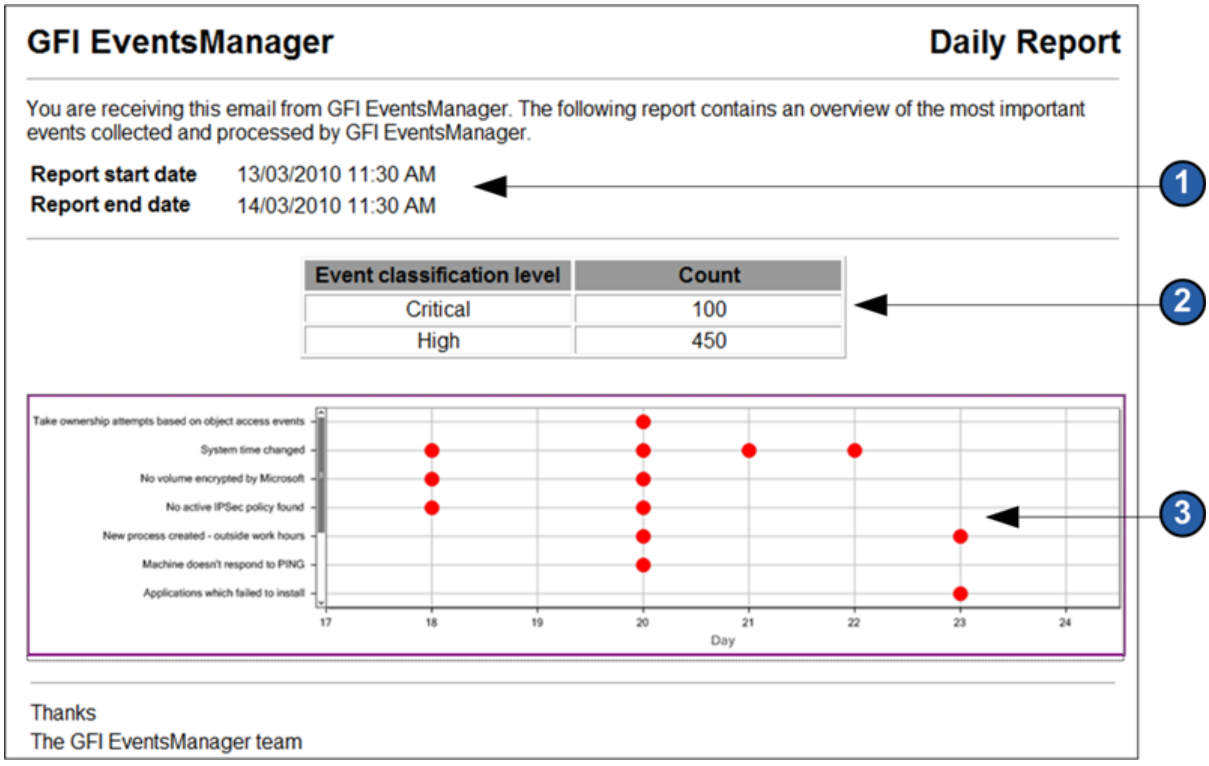


Screenshot 40 - Daily Digest email settings

5. Configure the time when the Daily Digest email is sent.

6. Click **OK**.

For more information on how to manage and create user accounts, refer to Configuring users and groups chapter in this manual.



Screenshot 41 - Daily digest emai

SECTION	DESCRIPTION
1	The start and end date of the report. The report displays the most important events collected by GFI EventsManager between the start and end date.
2	The number of Critical and High events collected in the last 24 hours.
3	This graph provides statistical information about critical events collected from all event sources in the last 24 hours. For more information on the graph contents, refer to Critical and High Importance events section in this manual.

5.3 Settings report

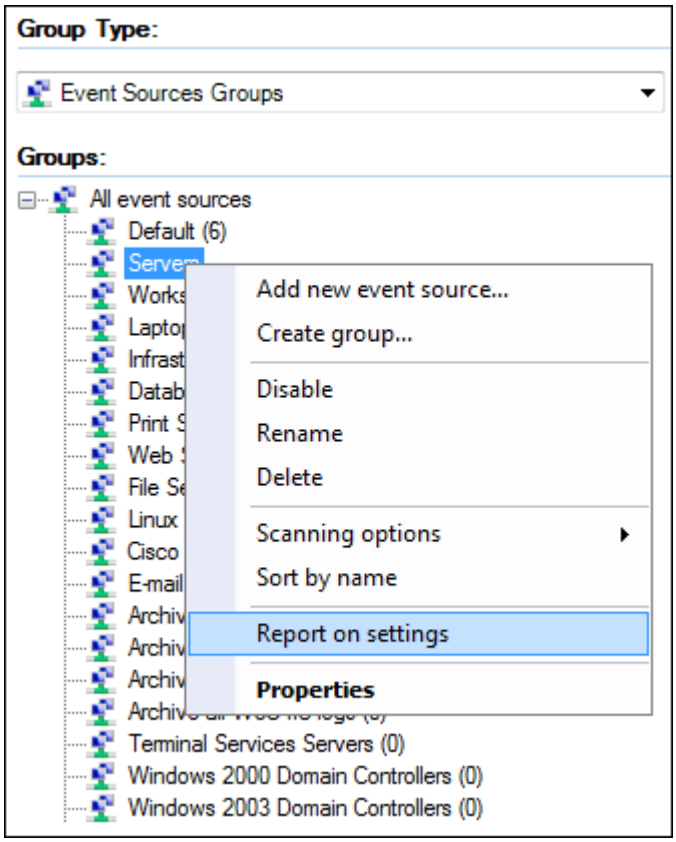
GFI EventsManager enables you to generate settings reports on event source groups. The provided information is described in Table 4 below:

Table 4 - Settings report heading information

HEADING	DESCRIPTION
Group name	The name of the group the report is based on.
Computer name	A list of every event source in the selected group.
Scan intervals	Scanning interval for every event source in the selected group; shown in Days : Hours : Minutes : Seconds.
Rules folder	Provides a list of rule categories applied to the selected group, such as: » Noise reduction » Security » System health » PCI DSS requirements
Rule sets	A granular list of rules applied on the selected group.

To generate settings report:

1. Click **Configuration** tab ► **Event Sources**.



Screenshot 42 - Generate configuration report

2. Right-click an event source group.

3. Click **Report on settings** and wait for report to generate.

GFI EventsManager — Monitored computers

Group name	Computer name	Scan interval (D.H:M:S)	Enabled	Rule folders	Rule sets
Workstations	W701	00:30:00	Yes	Noise Reduction	User-based noise,Defective logging noise,Over-logging noise,
				Security	Monitoring and attack detection,Windows Filtering Platform events,
				System Health	Disk issues,Memory dumps,TCP-IP issues,Unexpected system shutdowns,Applications crashing or hanging,Windows updates,Performance logs and alerts,Shutdown-reboot-logoff actions,
				Security Applications	Event logging system,Windows file protection,Windows firewall,Windows installer,Group Policy,
				GFI Rules	GFI LANguard rules,GFI EventsManager rules,GFI EndPointSecurity rules,
				Custom Rules	Custom
Workstations	W703	00:30:00	Yes	Noise Reduction	User-based noise,Defective logging noise,Over-logging noise,
				Security	Monitoring and attack detection,Windows Filtering Platform events,
				System Health	Disk issues,Memory dumps,TCP-IP issues,Unexpected system shutdowns,Applications crashing or hanging,Windows updates,Performance logs and alerts,Shutdown-reboot-logoff actions,
				Security Applications	Event logging system,Windows file protection,Windows firewall,Windows installer,Group Policy,
				GFI Rules	GFI LANguard rules,GFI EventsManager rules,GFI EndPointSecurity rules,
				Custom Rules	Custom

Screenshot 43 - Settings report sample

5.4 Rules report

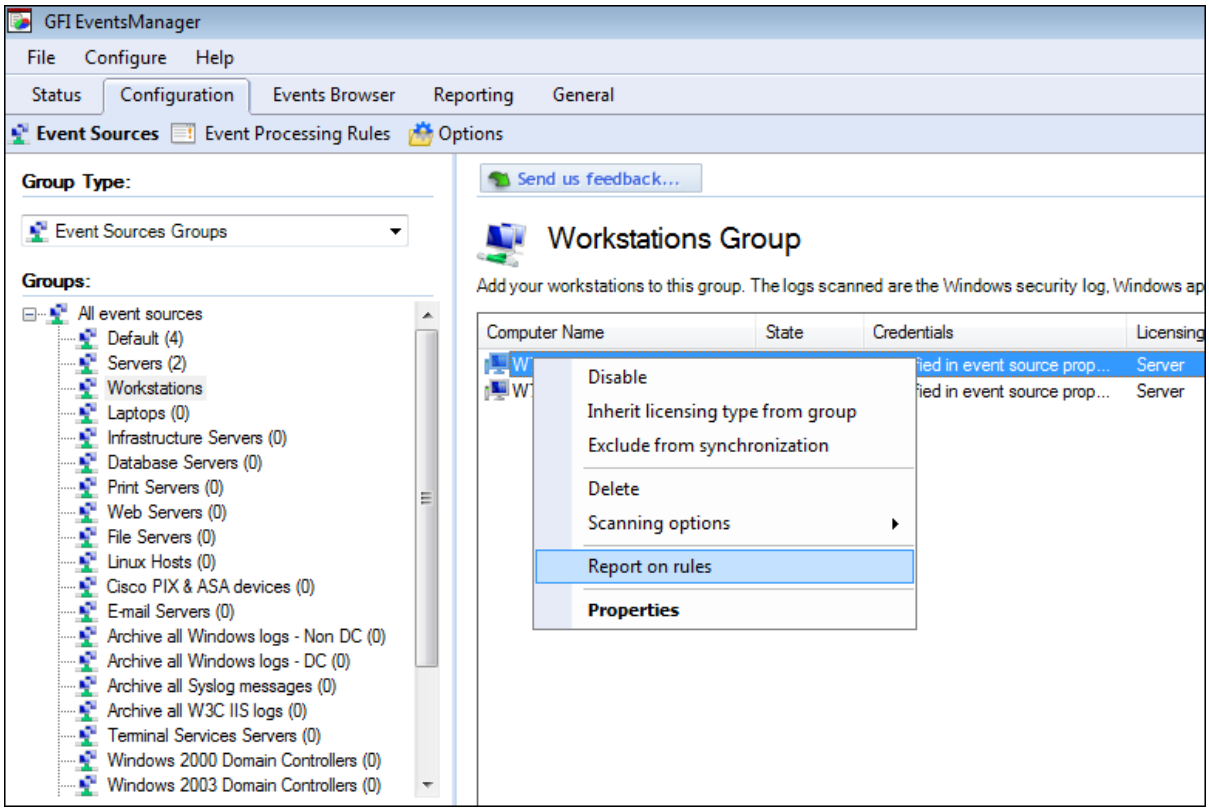
Rules repots provide a detailed view of applied rules on event sources. Table 5 below describes the rules report:

Table 5 - Rules report heading information

HEADING	DESCRIPTION
Rule name	Name of the applied rule.
Importance	The classified importance level of the collect event log, such as: » Critical » High » Medium » Low » Noise event.
Logfile monitored	Provides the category name of the collected event log, such as: » Security » System Health » Application » System.
Conditions	The processing condition(s) for the selected rule. This includes: » Event IDs » Source » Category » User » Type » Advanced.
Actions	Describes the actions taken when the event is processed, including: » Archiving settings » Mail to settings » Threshold settings.

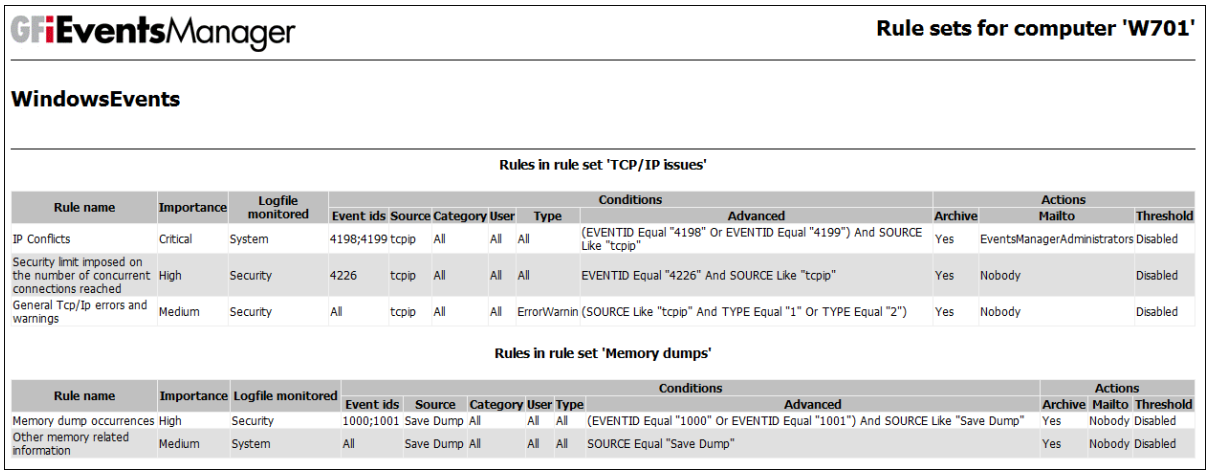
To generate rules report:

1. Click **Configuration** tab ► **Event Sources.**



Screenshot 44 - Generate configuration report

2. Right-click an event source and click **Report on rules.**


GFiEventsManager

Rule sets for computer 'W701'

WindowsEvents

Rules in rule set 'TCP/IP issues'

Rule name	Importance	Logfile monitored	Conditions						Actions		
			Event ids	Source	Category	User	Type	Advanced	Archive	Mailto	Threshold
IP Conflicts	Critical	System	4198;4199	tcpip	All	All	All	(EVENTID Equal "4198" Or EVENTID Equal "4199") And SOURCE Like "tcpip"	Yes	EventsManagerAdministrators	Disabled
Security limit imposed on the number of concurrent connections reached	High	Security	4226	tcpip	All	All	All	EVENTID Equal "4226" And SOURCE Like "tcpip"	Yes	Nobody	Disabled
General Tcp/Ip errors and warnings	Medium	Security	All	tcpip	All	All	ErrorWarnin	(SOURCE Like "tcpip" And TYPE Equal "1" Or TYPE Equal "2")	Yes	Nobody	Disabled

Rules in rule set 'Memory dumps'

Rule name	Importance	Logfile monitored	Conditions						Actions		
			Event ids	Source	Category	User	Type	Advanced	Archive	Mailto	Threshold
Memory dump occurrences	High	Security	1000;1001	Save Dump	All	All	All	(EVENTID Equal "1000" Or EVENTID Equal "1001") And SOURCE Like "Save Dump"	Yes	Nobody	Disabled
Other memory related information	Medium	System	All	Save Dump	All	All	All	SOURCE Equal "Save Dump"	Yes	Nobody	Disabled

Screenshot 45 - Generate configuration report

5.5 Operational history

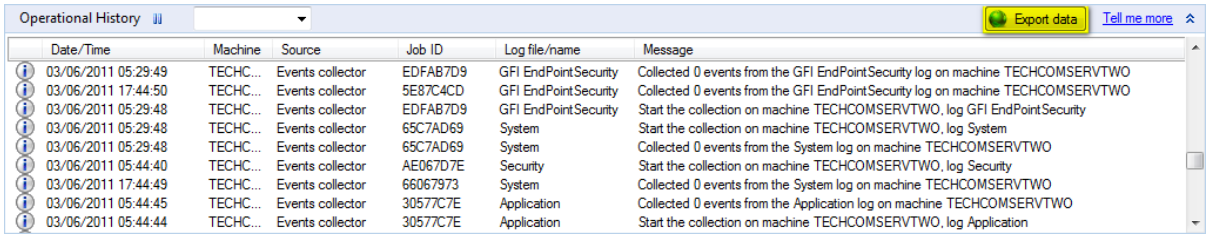
GFI EventsManager's operational history can be exported for further analysis and archiving purposes. Operational history messages provide administrators with information as described in Table 6 below:

Table 6 - Operational history reports

HEADING	DESCRIPTION
Date/Time	Date and time when the message was generated
Machine	Event source that generated the message
Source	Source operation that cause the message to be generated. Amongst others these include: » EvtCollector - message generated while collecting event logs » SNMP TrapsServer - message generated while collecting SNMP Traps Messages » EnetrpriseMaintenance - message generated during database maintenance jobs
Job ID	An internal ID associated with the job
Log file/name	Type of logs collected. Amongst others: » Application » Security » Logs generated by other applications such as GFI LANguard and GFI EndPointSecurity
Message	The actual message generated while performing the job.

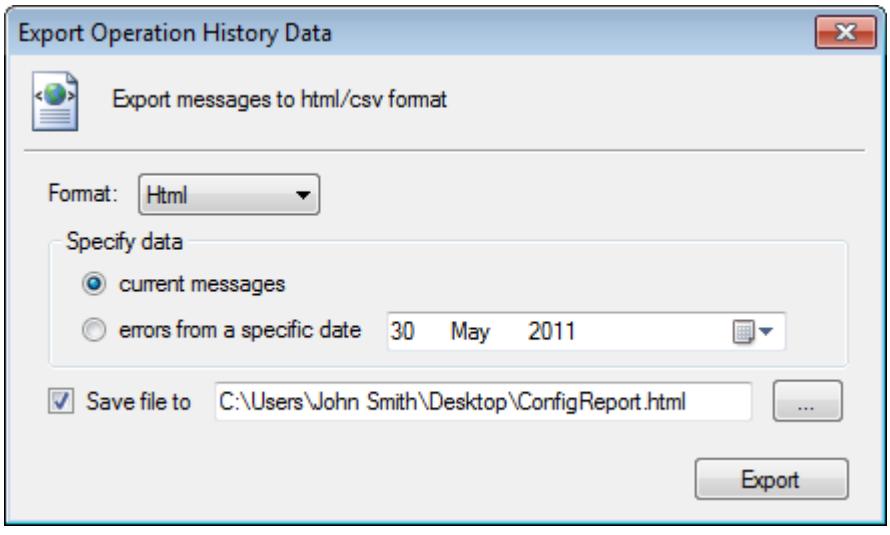
To generate Operational history reports:

1. From GFI EventsManager Management Console, click **Status ► Job Activity**.


Operational History
Export data
Tell me more
Date/Time Machine Source Job ID Log file/name Message
03/06/2011 05:29:49 TECHC... Events collector EDFAB7D9 GFI EndPointSecurity Collected 0 events from the GFI EndPointSecurity log on machine TECHCOMSERVTWO
03/06/2011 17:44:50 TECHC... Events collector 5E87C4CD GFI EndPointSecurity Collected 0 events from the GFI EndPointSecurity log on machine TECHCOMSERVTWO
03/06/2011 05:29:48 TECHC... Events collector EDFAB7D9 GFI EndPointSecurity Start the collection on machine TECHCOMSERVTWO, log GFI EndPointSecurity
03/06/2011 05:29:48 TECHC... Events collector 65C7AD69 System Start the collection on machine TECHCOMSERVTWO, log System
03/06/2011 05:29:48 TECHC... Events collector 65C7AD69 System Collected 0 events from the System log on machine TECHCOMSERVTWO
03/06/2011 05:44:40 TECHC... Events collector AE067D7E Security Start the collection on machine TECHCOMSERVTWO, log Security
03/06/2011 17:44:49 TECHC... Events collector 66067973 System Collected 0 events from the System log on machine TECHCOMSERVTWO
03/06/2011 05:44:45 TECHC... Events collector 30577C7E Application Collected 0 events from the Application log on machine TECHCOMSERVTWO
03/06/2011 05:44:44 TECHC... Events collector 30577C7E Application Start the collection on machine TECHCOMSERVTWO, log Application

Screenshot 46 - Operational history report

2. Click **Export data**.

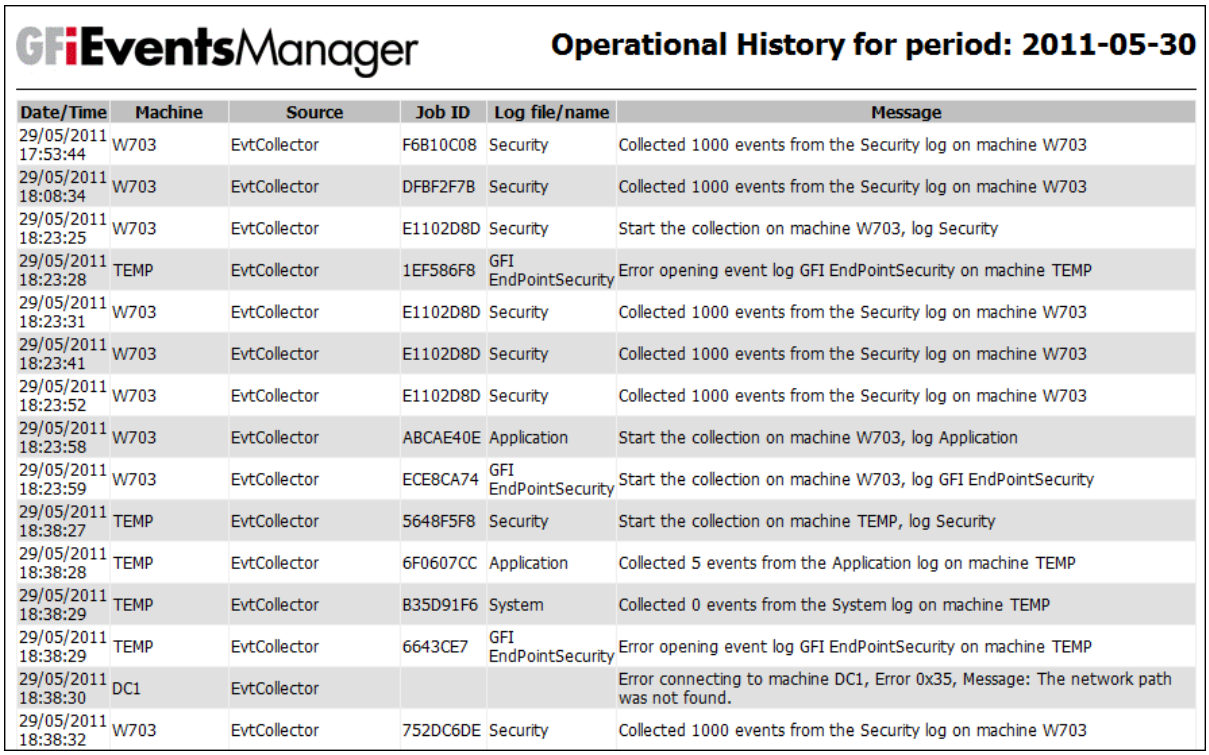


Screenshot 47 - Operational history dialog

3. Specify the options described in Table 7 below and click **Export**.

Table 7 - Export operational history options

OPTION	DESCRIPTION
Format	Select the report output format. Available formats are HTML and CSV.
Current messages	Export all messages displayed in **Job Activity** tab.
Errors from a specific date	Specify a date and export all the messages generated on that date.
Save file to	Select checkbox to specify output location. If not selected, reports are saved in the default location within the GFI EventsManager directory.



GFI EventsManager **Operational History for period: 2011-05-30**

Date/Time	Machine	Source	Job ID	Log file/name	Message
29/05/2011 17:53:44	W703	EvtCollector	F6B10C08	Security	Collected 1000 events from the Security log on machine W703
29/05/2011 18:08:34	W703	EvtCollector	DFBF2F7B	Security	Collected 1000 events from the Security log on machine W703
29/05/2011 18:23:25	W703	EvtCollector	E1102D8D	Security	Start the collection on machine W703, log Security
29/05/2011 18:23:28	TEMP	EvtCollector	1EF586F8	GFI EndPointSecurity	Error opening event log GFI EndPointSecurity on machine TEMP
29/05/2011 18:23:31	W703	EvtCollector	E1102D8D	Security	Collected 1000 events from the Security log on machine W703
29/05/2011 18:23:41	W703	EvtCollector	E1102D8D	Security	Collected 1000 events from the Security log on machine W703
29/05/2011 18:23:52	W703	EvtCollector	E1102D8D	Security	Collected 1000 events from the Security log on machine W703
29/05/2011 18:23:58	W703	EvtCollector	ABCAE40E	Application	Start the collection on machine W703, log Application
29/05/2011 18:23:59	W703	EvtCollector	ECE8CA74	GFI EndPointSecurity	Start the collection on machine W703, log GFI EndPointSecurity
29/05/2011 18:38:27	TEMP	EvtCollector	5648F5F8	Security	Start the collection on machine TEMP, log Security
29/05/2011 18:38:28	TEMP	EvtCollector	6F0607CC	Application	Collected 5 events from the Application log on machine TEMP
29/05/2011 18:38:29	TEMP	EvtCollector	B35D91F6	System	Collected 0 events from the System log on machine TEMP
29/05/2011 18:38:29	TEMP	EvtCollector	6643CE7	GFI EndPointSecurity	Error opening event log GFI EndPointSecurity on machine TEMP
29/05/2011 18:38:30	DC1	EvtCollector			Error connecting to machine DC1, Error 0x35, Message: The network path was not found.
29/05/2011 18:38:32	W703	EvtCollector	752DC6DE	Security	Collected 1000 events from the Security log on machine W703

Screenshot 48 - Operational history report sample

5.6 Activity overview

GFI EventsManager enables you to export **Activity Overview** data. Activity overview reports provide the information described in Table 8 below:

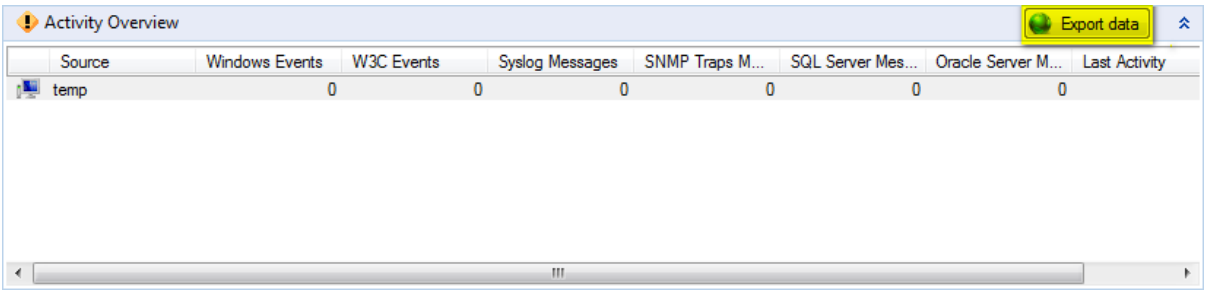
Table 8 - Activity overview headings

HEADING	DESCRIPTION
Date/Time	Date and time when the message was generated
Machine	Event source that generated the message
Source	Source operation that cause the message to be generated. Amongst others these include: » EvtCollector - message generated while collecting event logs » SNMP TrapsServer - message generated while collecting SNMP Traps Messages » EnetrpriseMaintenance - message generated during database maintenance jobs
Job ID	An internal ID associated with the job

HEADING	DESCRIPTION
Log file/name	Type of logs collected. Amongst others: » Application » Security » Logs generated by other applications such as GFI LANguard and GFI EndPointSecurity
Message	The actual message generated while performing the job.

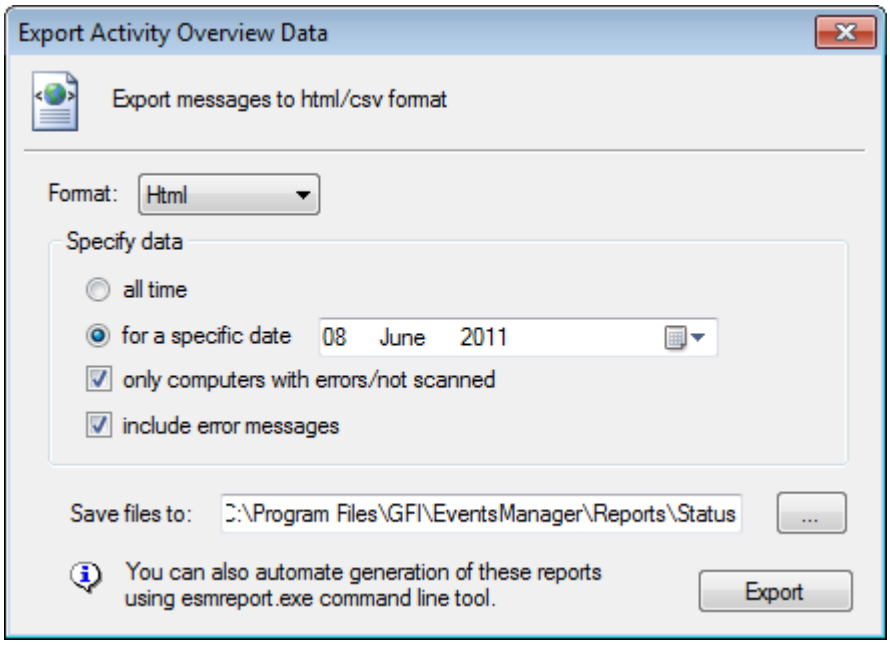
To export **Activity Overview**:

1. From GFI EventsManager Management Console, click **Status ► Statistics**.



Screenshot 49 - Activity overview button

2. Click **Export data**.



Screenshot 50 - Activity overview dialog

3. Configure the options described in and click **Export**.

Table 9 - Export operational history options

OPTION	DESCRIPTION
Format	The report output format. Available formats are HTML and CSV.
All time	Export all messages displayed **Activity Overview**.
From a specific date	Specify a date to export all messages generated on that date.
Only computers with errors/	Export only data of computers with scanning issues.
Include error messages	Select this option to include the generated error message.
Save files to	Displays the default export location.

GFI EventsManager

Activity Overview for period: 2011-06-08

Source	Windows Events	W3C Events	Syslog Messages	SNMP Traps Messages	SQL Server Messages	Oracle Server Messages	Last Activity
192.168.3.20	9502	0	0	0	0	0	08/06/2011 23:52:08
w701	0	0	0	0	0	0	No Activity

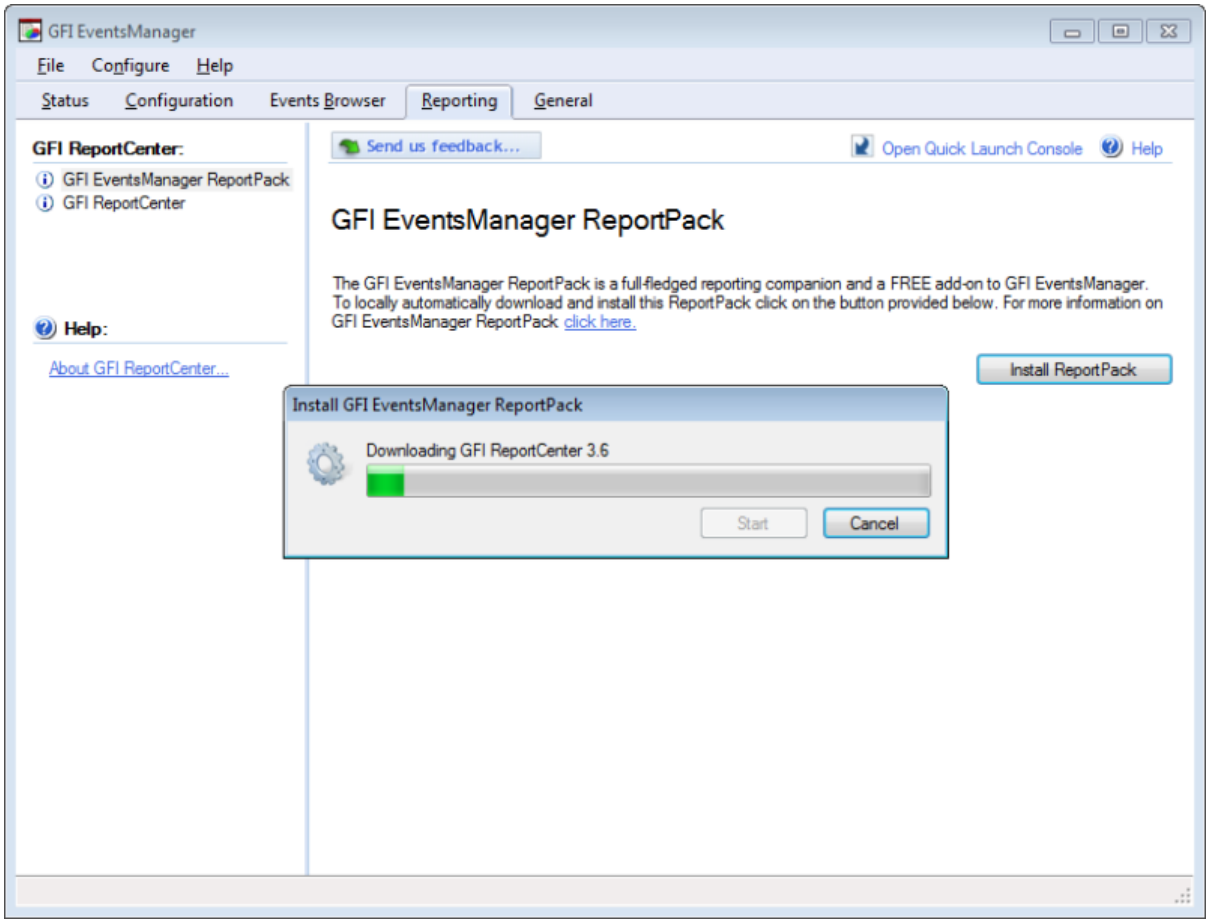
Operational History for period: 2011-06-08

Date/Time	Type	Machine	Source	Job ID	Log file/name	Message
08/06/2011 23:51:40	Error	w701	EvtCollector			Error connecting to machine w701, Error 0x5, Message: Access is denied.
08/06/2011 23:51:49	Error	w701	EvtCollector			Error connecting to machine w701, Error 0x5, Message: Access is denied.

Screenshot 51 - Activity overview report sample

5.7 Download the GFI EventsManager ReportPack

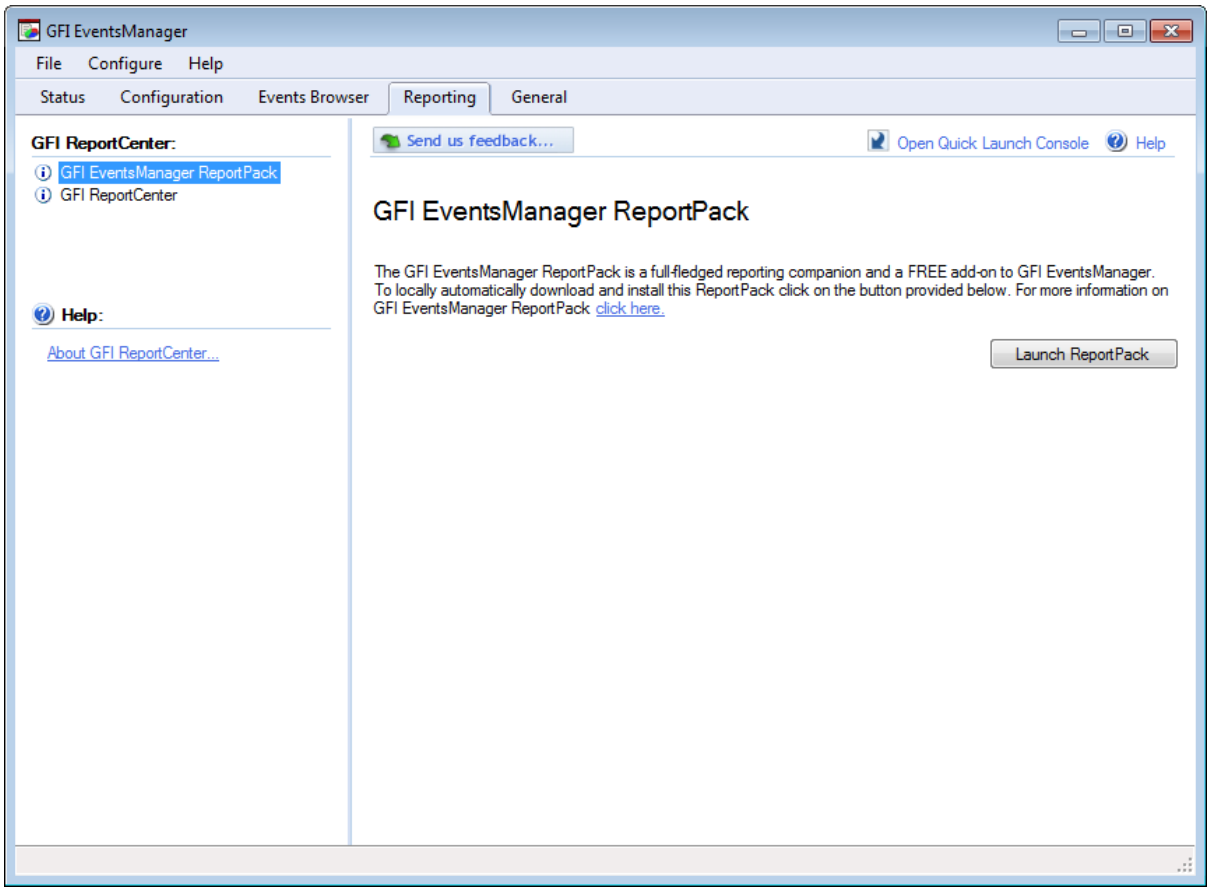
From GFI EventsManager **Reporting** tab, click **Install ReportPack** button to download and install the GFI EventsManager ReportPack on the local machine. Prior to installing the GFI EventsManager ReportPack, GFI EventsManager will also prompt you to install any pre-requisites that are required. This includes the GFI ReportCenter framework.



Screenshot 52 - Downloading GFI EventsManager ReportPack

For installation instructions and more information about the GFI EventsManager ReportPack refer to GFI EventsManager ReportPack manual, available at: http://www.gfi.com/eventsmanager/esm2011rpmanual.pdf.

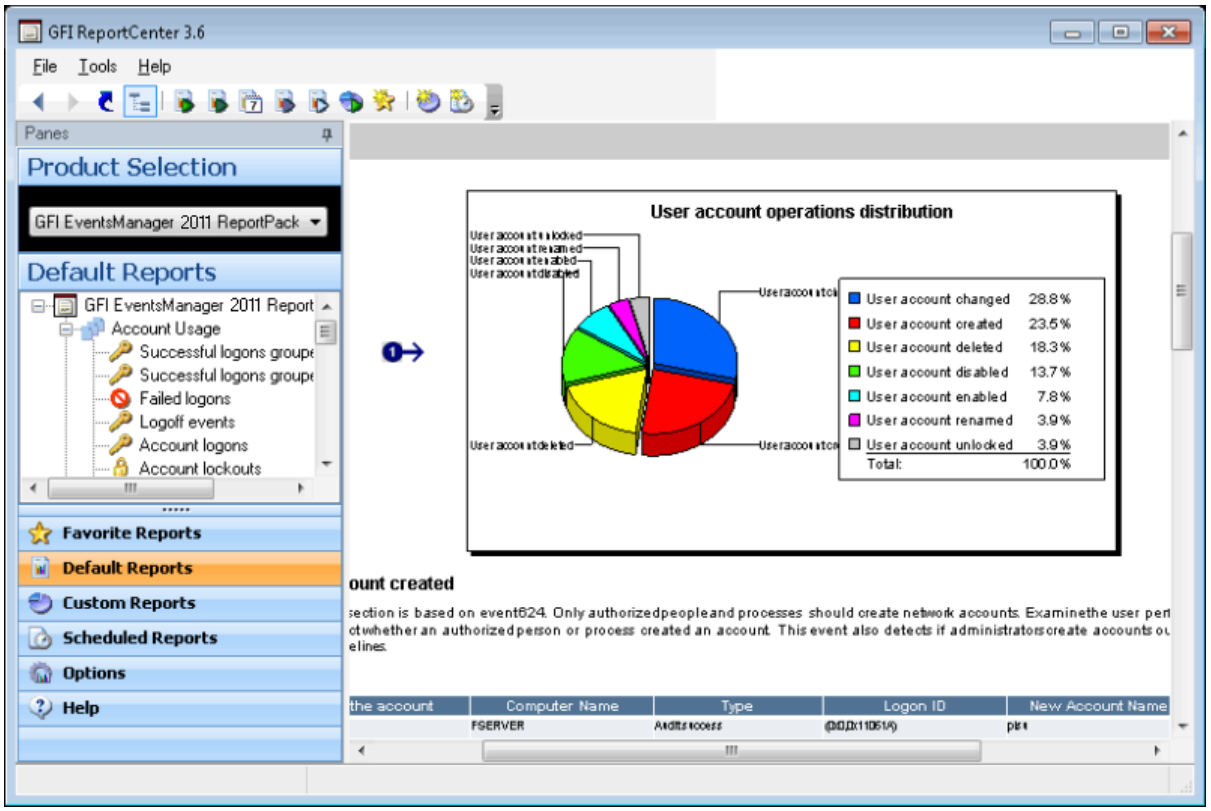
5.8 Launching the GFI EventsManager ReportPack



Screenshot 53 - Launching the GFI EventsManager ReportPack

To generate reports:

1. Click **Launch ReportPack** button



Screenshot 54 - GFI EventsManager ReportPack console

2. The GFI EventsManager ReportPack console will open in a new window.

For more information about the reports and the functionalities of GFI EventsManager ReportPack refer to GFI EventsManager ReportPack manual, available at: http://www.gfi.com/eventsmanager/esm2011rpmanual.pdf.

6 Manage event sources

6.1 Introduction

An event source is a network computer that is accessed and processed by GFI EventsManager. In GFI EventsManager, these event sources are organized into specific computer groups. The **Event Sources** tab enables you to organize event sources to suit your network infrastructure. You can create new or use default groups to distinctively organize and configure the servers, workstations and laptops that will be monitored by GFI EventsManager.

6.2 Managing event sources groups

Event sources are organized in groups. Grouping events enables you to configure common actions and settings for multiple computers within the group. GFI EventsManager ships with pre-configured groups and in addition enables you to create your custom groups.

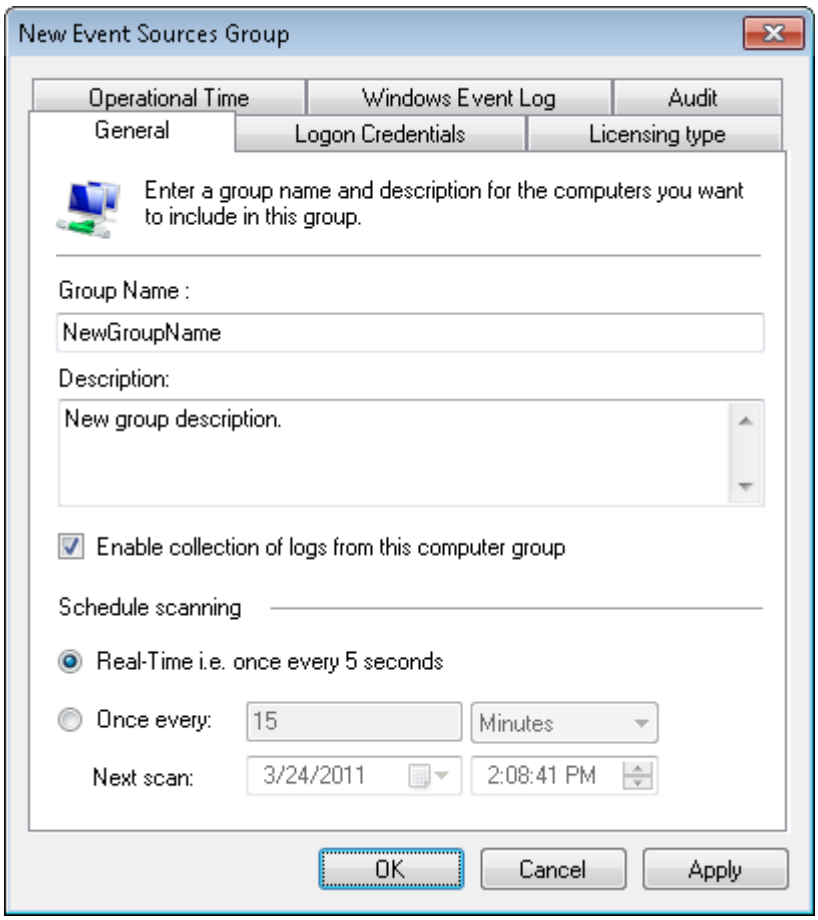
6.2.1 Create a new group

To create a new event source group:

1. Click **Configuration** tab ► **Event Sources** and from **Group Type** select **Event Sources Groups**.

2. Right click **All event sources** and select **Create group…**

3. Select the license type to use, between **Workstation** and **Server** license.



Screenshot 55 - Add new event source group

4. Key-in a valid name and a description(optional). Select the tabs described in Table 10 below, and configure the available options.

Table 10 - Event source group options

TAB NAME	DESCRIPTION
General	Enable collection of events and schedule the scanning process. For more information, refer to Configuring general event source properties section in this manual.
Logon credentials	Configure the username and password used to login target machines and collect information. For more information, refer to Configure Logon Credentials section in this manual.
Licensing type	Select the type of license to use. Select between workstation and server license.
Operational time	Configure the operational time that computers are normally used. For more information, refer to Configure operational time section in this manual.
Windows Event Log	Specify the logs to collect and configure archive settings for Windows event logs. For more information, refer to Collecting Windows events section in this manual.
Audit	Enable GFI EventsManager auditing on target computers and configure the audit to perform. For more information, refer to Configure GFI EventsManager Auditing section in this manual.
W3C Logs	Specify the logs to collect and configure archive settings for W3C logs. This tab is only available when creating a server group. For more information, refer to Collecting W3C logs section in this manual.
Syslog	Specify the logs to collect and configure archive settings for Syslogs. This tab is only available when creating a server group. For more information, refer to Collecting Syslogs section in this manual.
SNMP Traps	Specify the logs to collect and configure archive settings for SNMP Traps. This tab is only available when creating a server group. For more information, refer to Collecting SNMP Traps section in this manual.

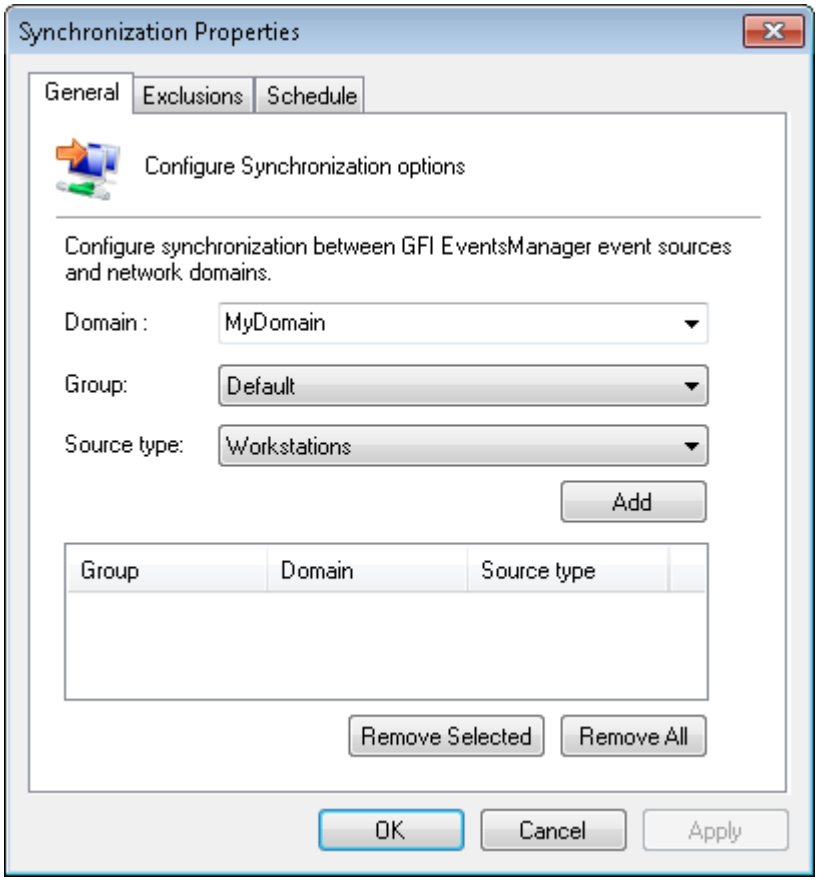
5. Click **OK** to save changes.

6.2.2 Edit synchronization options

GFI EventsManager enables you to synchronize domains with event sources groups. When the synchronization is configured, the domain members will be added automatically to GFI EventsManager event sources. To edit synchronization options:

1. Select **Configuration** tab and from **Group Type**, select **Event Sources Groups**.

2. Select **All event sources** node. From **Actions,** click **Edit synchronization options**.



Screenshot 56 - Synchronization properties - General tab

3. Select **General** tab and configure the options described in Table 11 below.

Table 11 - Synchronization properties - General tab

OPTION	DESCRIPTION
Domain	Select the domain name from the list or key-in a valid domain name.
Group	Select the GFI EventsManager group name where to add the discovered event sources.
Sync with	Select the type of computers discovered in the selected domain that will be added to the selected GFI EventsManager group.

4. To include the synchronization click **Add**.

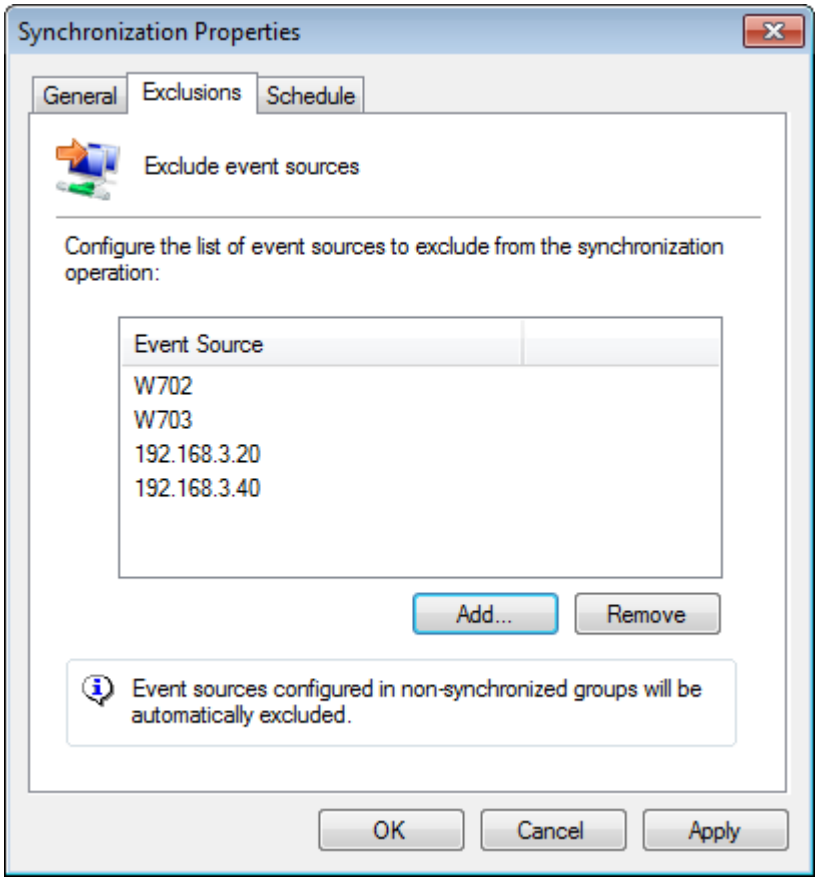
5. Repeat steps 3 to 4 for each synchronization. Table 12 below shows some examples of possible synchronizations that can be configured.

Table 12 - Example of synchronizations

GROUP	SYNC WITH
Archive all Windows logs-Non DC	Generic Servers
Workstations	Workstations
E-mail Servers	Exchange Servers
Archive all Windows logs - DC	Domain Controllers
Servers	ISA Servers

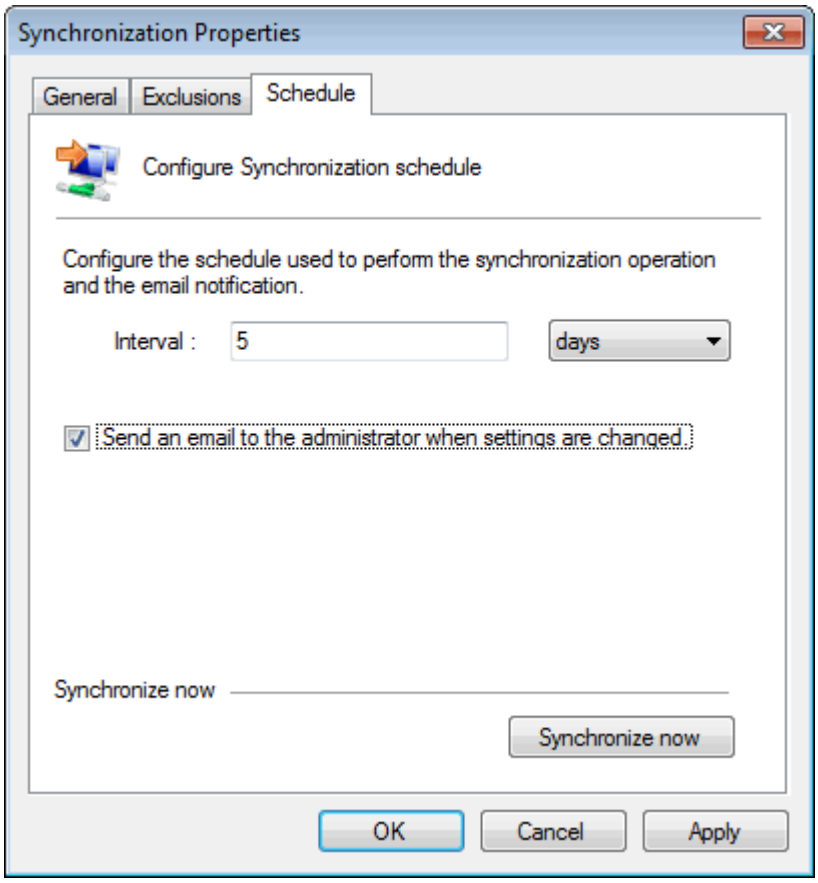
6. (Optional) Select **Exclusions** tab to configure the list of computers that will be excluded from the synchronization. Click Add and key-in a computer name to exclude.

Event sources that are already part of an event source group will be automatically excluded from synchronization. For more information on how to manage event source groups, refer to Manage event sources chapter in this manual.



Screenshot 57 - Synchronization properties - Exclusion tab

7. Select **Schedule** tab to configure when the synchronization should be performed.



Screenshot 58 - Synchronization properties -Schedule tab

8. Key-in a valid interval in hours or days.

9. (Optional) Select **Send an email to the…** to send an email notification when event sources are changed after synchronization.

10. (Optional) Click **Synchronization now** to synchronize event sources immediately.

11. Click **OK**.

Adding Event Sources manually to a synchronized group is not allowed in GFI EventsManager.

6.3 Adding event sources

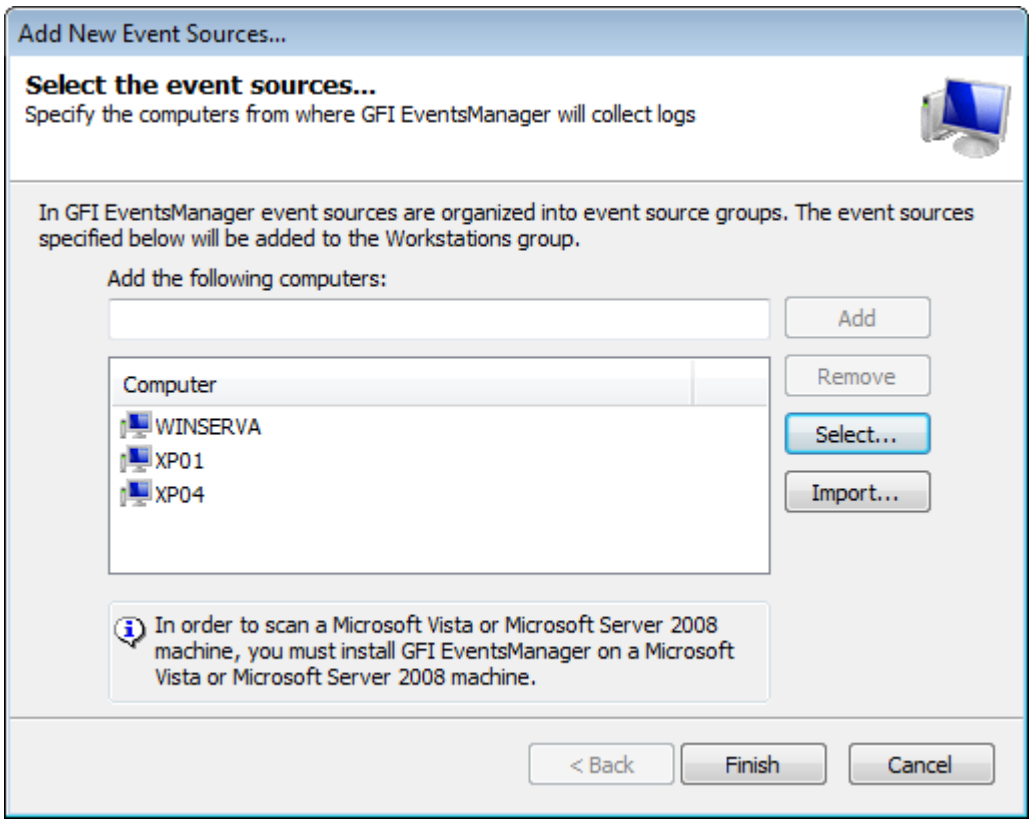
6.3.1 Adding an event source to a group

To add a new event sources to a computer group:

1. Click **Configuration** tab ► **Event Sources**.

2. From **Group Type**, select **Event Sources Groups**.

3. Right-click Computer Group which will contain the new event sources and select **Add new event source**.

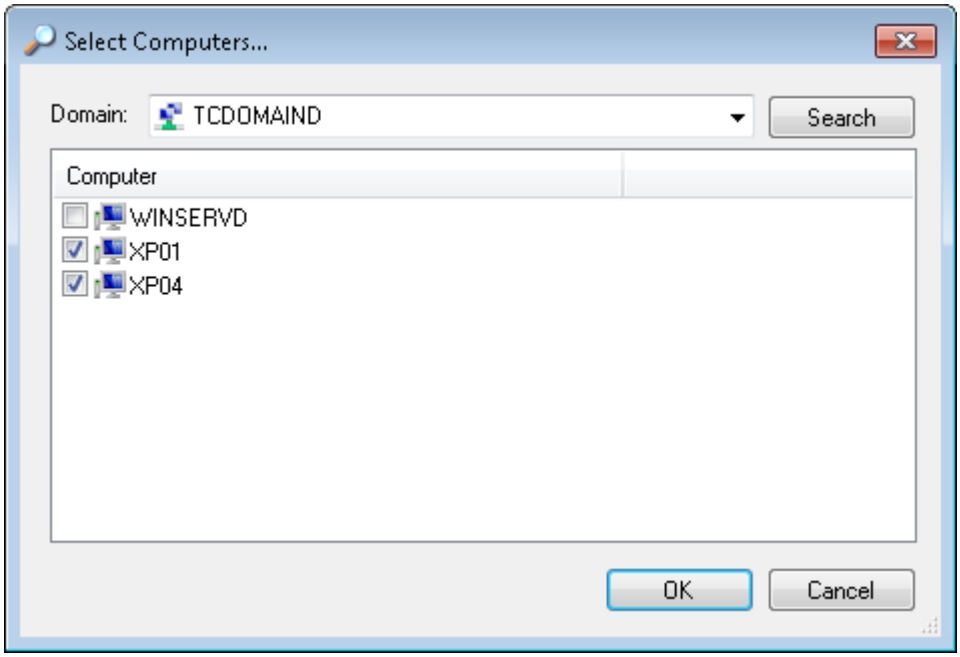

Add New Event Sources...
Select the event sources...
Specify the computers from where GFI EventsManager will collect logs
In GFI EventsManager event sources are organized into event source groups. The event sources specified below will be added to the Workstations group.
Add the following computers:
Add
Computer
Remove
WINSERVA
XP01
XP04
Select...
Import...
In order to scan a Microsoft Vista or Microsoft Server 2008 machine, you must install GFI EventsManager on a Microsoft Vista or Microsoft Server 2008 machine.
< Back
Finish
Cancel

Screenshot 59 - Configuration wizard: Specify the computers that will be monitored

4. Specify the name/IP of the new event source and click **Add**. Repeat until you have specified all the event sources to add to this group.

Since Syslog and SNMP traps use the IP address to determine the source of an event, it is recommended to use the source IP instead of the domain name when retrieving Syslog and SNMP traps from target machines.

5. (Optional) Click **Select** to browse the network for existing domains and computers. Select the domain from the **Domain** drop down list and select the computers to add.



Screenshot 60 - Browse the network for connected computers

To import the list of event sources from a text file click **Import** button.

6. Click **Finish** to finalize your settings. GFI EventsManager will attempt to collect logs from the configured sources immediately.

If synchronization is not enabled, you can use the **Network Discovery Wizard** to automatically search and add events sources. To launch Network Discovery Wizard, click **Scan local domain** under **Common Tasks**. For more information on how to use the Network discovery wizard, refer to Processing events from the local domain section in this manual.

6.4 Configuring event source properties

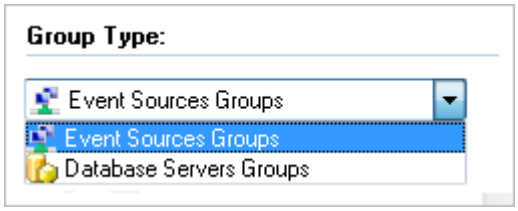
GFI EventsManager allows you to customize the event source parameters to suit the operational requirements of your infrastructure. You can configure these parameters on a:

Computer by computer basis.

Group by group basis.

To configure event source properties:

1. Click **Configuration** tab.



Screenshot 61 - Group type

2. From **Group Type**, select **Event Sources Groups**.

3. To configure the parameters of:

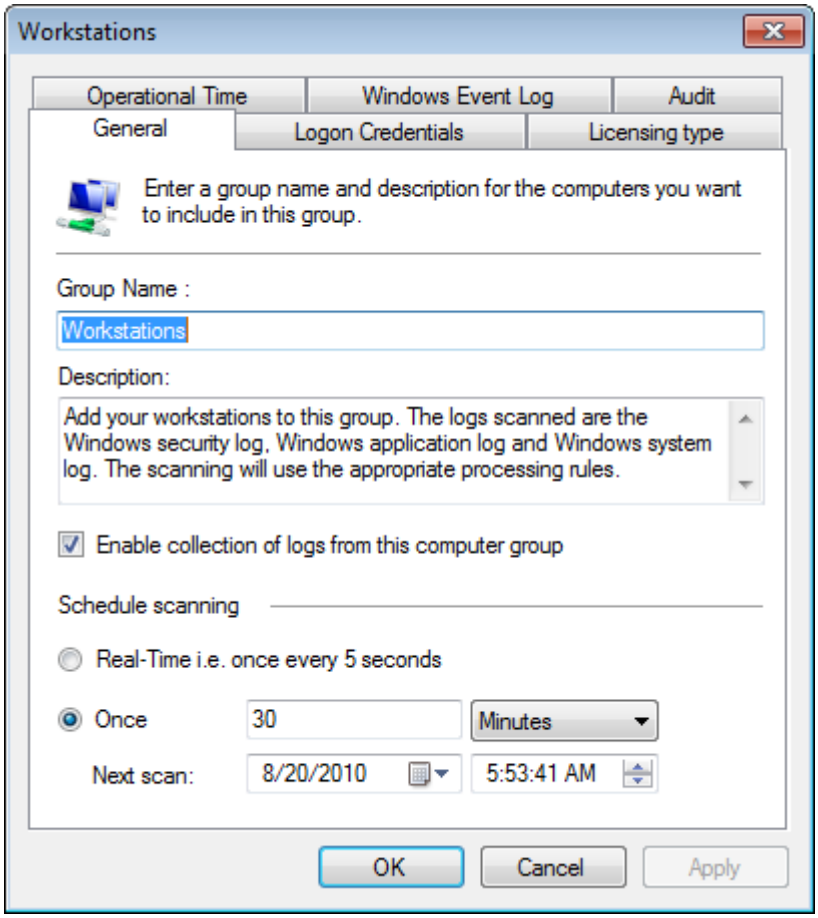
» Computer group: Right-click on the computer group to be configured and select **Properties**.

» Particular computer in a group:

- Click on the computer / database server group to which the computer group belongs.
- From the right pane, right-click on the required computer and select **Properties**.

4. Click required tabs and configure the respective parameters accordingly. More information on how to configure these parameters is provided in this chapter.

6.4.1 Configuring general event source properties



Screenshot 62 - Event sources properties dialog

Use the **General** tab in the properties dialog to:

Change the name of a computer group.

Enable/disable log collection and processing for the computers in a group.

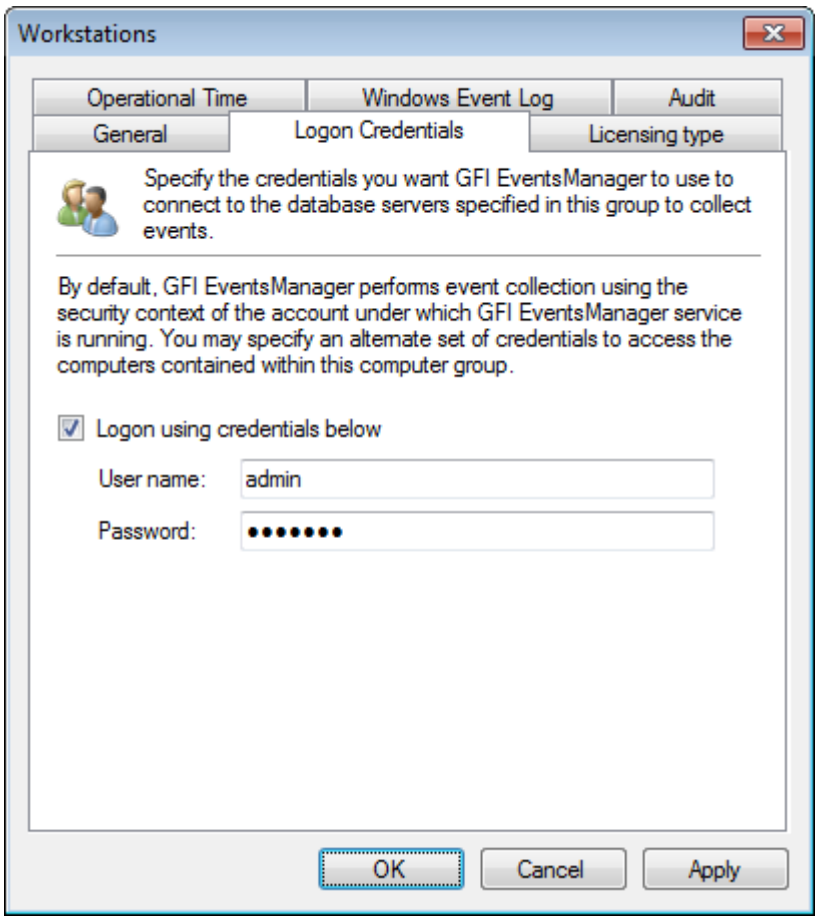
Configure log collection and processing frequency.

6.4.2 Configure Logon Credentials

During event processing, GFI EventsManager must remotely log-on to the target computers. This is required in order to collect log data that is currently stored on the target computers and to pass this data on to the event processing engine(s).

To collect and process logs, GFI EventsManager must have administrative privileges over the target computers. By default, GFI EventsManager will log-on to target computers using the credentials of the account under which it is currently running; however, certain network environments are configured to use different credentials to log on to workstations and servers with administrative privileges. As an example for security purposes, network

administrators can setup a dedicated account that has administrative privileges over workstations only and a different account that has administrative privileges over servers only.


Workstations
Operational Time
Windows Event Log
Audit
General
Logon Credentials
Licensing type
Specify the credentials you want GFI EventsManager to use to connect to the database servers specified in this group to collect events.
By default, GFI EventsManager performs event collection using the security context of the account under which GFI EventsManager service is running. You may specify an alternate set of credentials to access the computers contained within this computer group.
Logon using credentials below
User name:
admin
Password:
OK
Cancel
Apply

Screenshot 63 - Configuring alternative logon credentials

GFI EventsManager, allows you to configure a dedicated set of logon credentials for individual target computers as well as for computer groups. To configure a set of credentials for a particular computer group:

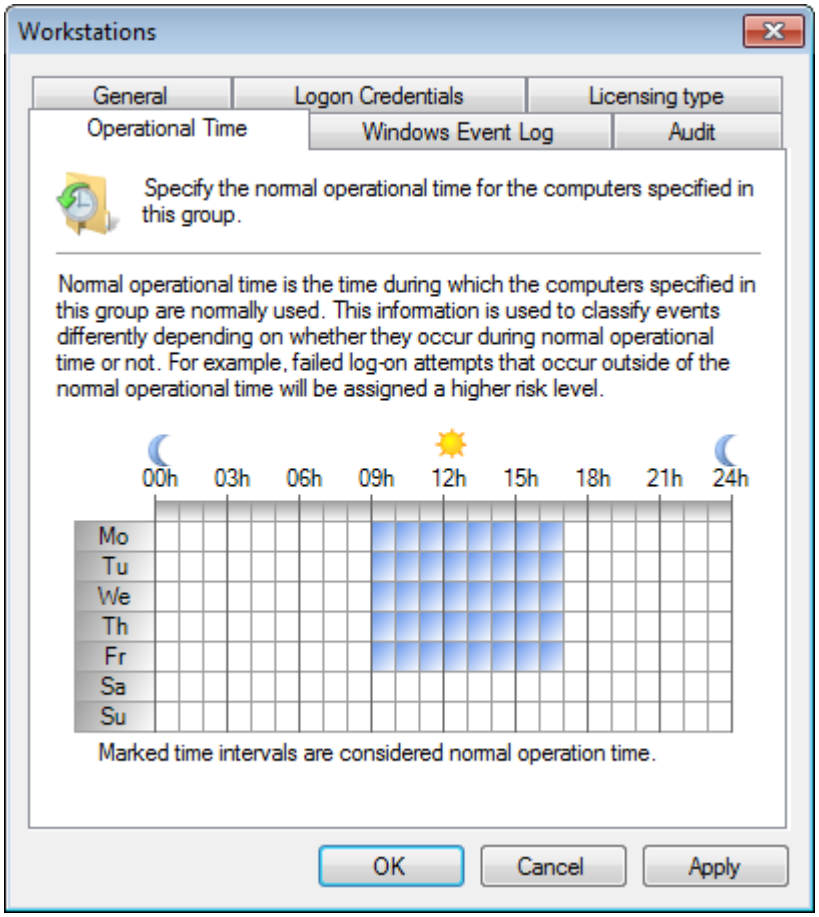
1. Right click on an event source and click on **Properties**

2. Click **Logon Credentials** tab

3. Specify the login name and password which will be used to log-on and collect logs from the target computer(s).

6.4.3 Configure operational time

GFI EventsManager includes an **Operational Time** option through which you specify the normal working hours of your event sources. This is required so that GFI EventsManager can keep track of the events that occur both during and outside working hours. Use the operational time information for forensic analysis and to identify network computers that are being misused outside normal working hours. For example, through this information, you can discover unauthorized user access, illicit transactions carried out outside normal working hours and other potential security breaches that might be taking place on your network.



Screenshot 64 - Specify operational time

Operational time is configurable on computer group basis. Configuration is achieved through the **Operational Time** tab provided in the computer group properties; Operational time is configured by marking the normal working hours on a graphical operational time scale which is divided into 1 hour segments.

6.4.4 Configure GFI EventsManager Auditing

GFI EventsManager can collect additional data from the network using a checking engine. If auditing is enabled on an event source, the audit will be executed before collecting events and creates relative Windows events.

For example, when executing **Check slow connection**, the script performs a PING request and records the response time. If the response time is more than 500 milliseconds, the script creates a Windows event in the Application log of the target machine.

If an audit fails to execute due to network disconnection or insufficient permissions, no windows events are created.

CHECK LIST	DESCRIPTIONS
Check audit policy	Checks the status of audit policies on target machines. If an audit policy is disabled, a Windows event is created. For more information on how to enable audit policies, refer to Step 2: Enable additional auditing features section in this manual.
Check disk space	Checks the target machine disk drives' free space. If a disk has less than 10% free space, a Windows event is created. Amongst others, the Windows event contains information on disk drive name and storage space.
Check inactive domain machines	Checks the domain for inactive machines. A machine can be inactive if no log in requests were sent during the previous 30 days. If inactive machines are found, a Windows event is created.
Check inactive users	Checks domain for inactive user accounts. A user account is inactive if no log in requests were sent during the previous 30 days. If inactive accounts are found, a Windows event is created.

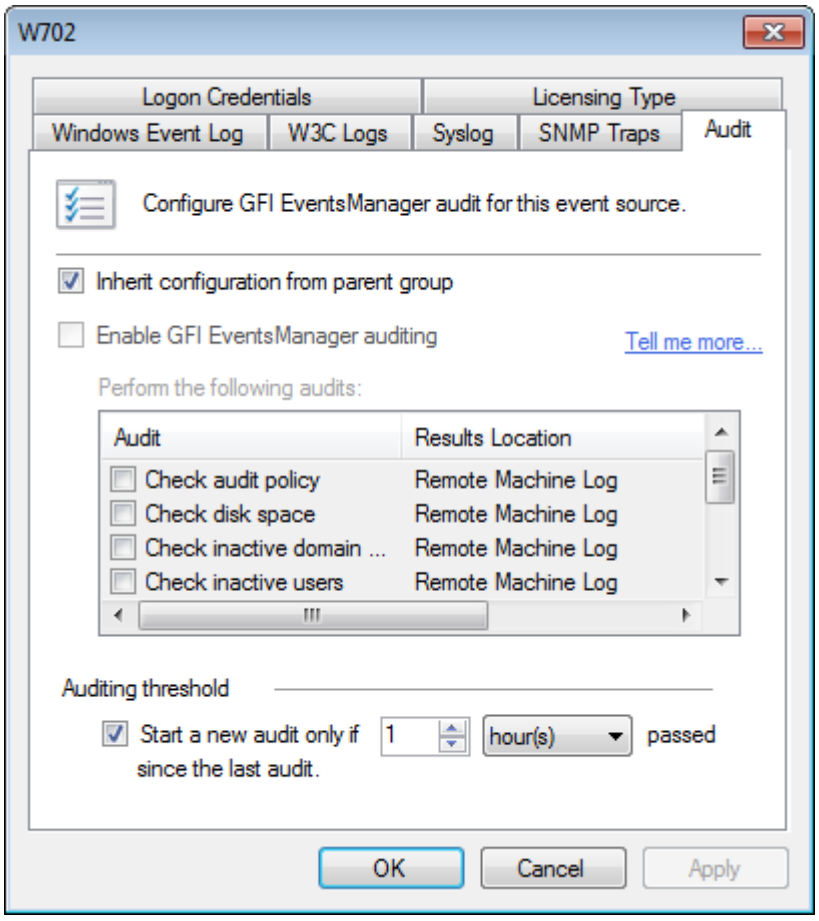
CHECK LIST	DESCRIPTIONS
Check IPSec policies status	Checks status of IPSec policies on target machines, if any. If IPSec policies exist and are inactive, a Windows event is created.
Check Microsoft firewall status	Checks status of any Microsoft Windows Firewall or ISA servers on target machines. If a Firewall exists and is off, a Windows event is created.
Check slow connection	The script performs a PING request and records the response time. If the response time is more than 500 milliseconds, the script creates a Windows event.
Check volumes encrypted by Microsoft	Checks if there are volumes encrypted using Microsoft products (e.g. Bit Locker), on target machines. If volume encryption is not used, a Windows event is created.

To configure GFI EventsManager auditing event processing rules, navigate to **Configuration** tab ► **Event Processing Rules** and from the left pane select **GFI Rules** ► **GFI EventsManager rules**. For more information on event processing rules, refer to Using event processing rules chapter in this manual.

To enable and configure GFI EventsManager auditing:

1. Right-click an event source or an event source group, and click **Properties**.

2. From the **Properties** dialog, select **Audit** tab.



Screenshot 65 - GFI EventsManager audit

3. Configure the options described in Table 13 below.

Table 13 - Auditing options

OPTION	DESCRIPTION
Inherit configuration from parent group.	Select this option to use the settings configured in the parent group.
Enable GFI EventsManager auditing	Select this option to enable GFI EventsManager auditing.

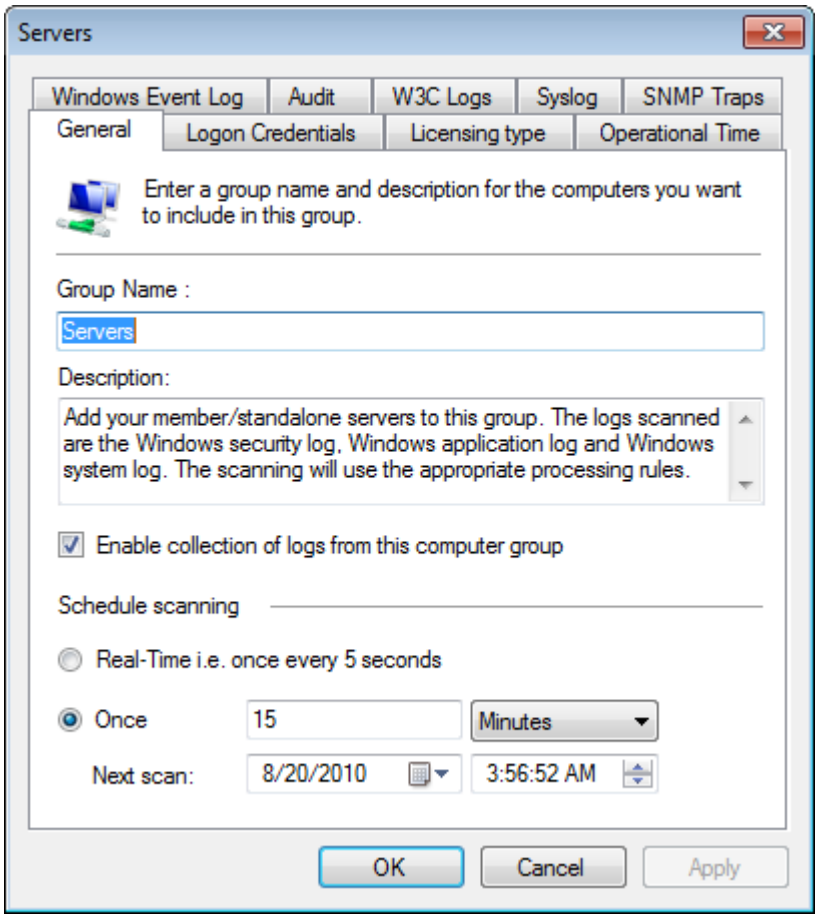
OPTION	DESCRIPTION
Perform the following audits	Select the audits to perform on target machines.
Start a new audit only if…	Select this option and configure the threshold time between audits. GFI EventsManager will wait for the defined interval before starting a new audit check.

Audit checks are executed before scanning windows events, if the audit check is successful a windows log event is created on the target machine. This may create a large number of events and it is recommended to configure and use the **Auditing threshold**. When using the **Auditing threshold** GFI EventsManager will wait for a pre-defined interval before starting a new audit check.

4. Click **OK** to save changes.

6.4.5 Configuring event processing parameters

To configure event processing parameters:



Screenshot 66 - Event-processing configuration tabs

1. Select the **Configuration** tab.

2. From the **Groups** list, right click the group to be configured and select **Properties**.

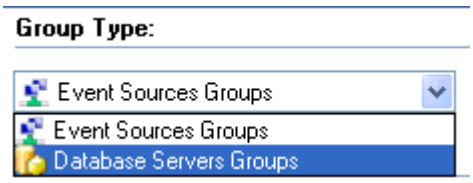
3. Use the **Windows Event Log** tab, **W3C Logs** tab, **Syslog** tab and **SNMP Traps** to configure the required event processing parameters. For more information on why and how to configure these parameters refer to Using event processing rules chapter.

6.5 Microsoft SQL Server sources

6.5.1 Adding a new Microsoft SQL Server group

To add a new Microsoft SQL Server group:

1. Click **Configuration** tab ► **Event Sources**. From **Group Type**, select **Database Servers Groups**.



Screenshot 67 - Database Servers Groups

2. From **Groups**, right-click **Microsoft SQL Servers** and select **Create group**.

3. Select **Microsoft SQL Server** as the server type and from the **General** tab configure the options described in Table 14 below:

Table 14 - Microsoft SQL Database group - General tab

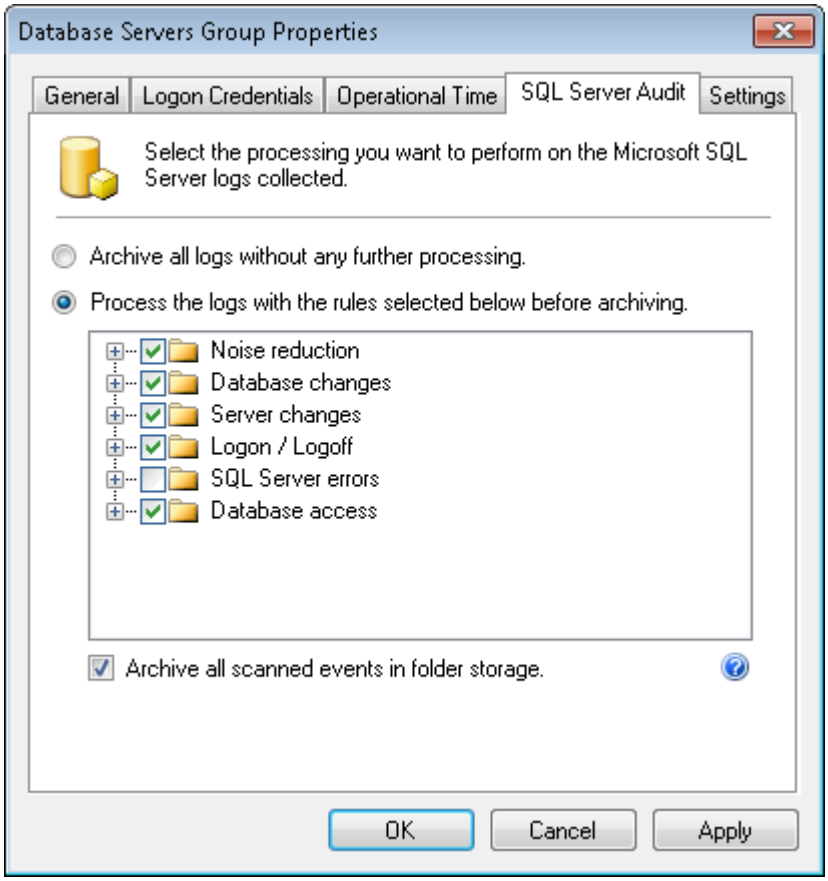
OPTION	DESCRIPTION
Group Name	Key in a group name to identify the Microsoft SQL server group.
Description	(Optional) Key-in a description.
Collects logs from the database servers included in this group.	Enable option to collect database events from all servers in this group.

4. Select **Logon Credentials** tab and configure the options described in Table 15 below.

Table 15 - Microsoft SQL Database group - Logon Credentials

OPTION	DESCRIPTION
Use Windows authentication	Connect to the Microsoft SQL Database using windows authentication.
Use SQL Server authentication	Connect to Microsoft SQL Database using a Microsoft SQL Database user account. Key in a username and password.

5. Select **Operational Time** and configure the normal operational time, when the database is normally used.



Screenshot 68 - Microsoft SQL Database group - SQL Server Audit tab

6. Select **SQL Server Audit** tab and configure the options described in Table 16 below.

Table 16 - Microsoft SQL Database group -SQL Server Audit

OPTION	DESCRIPTION
Archive all logs without further processing	Archive events in GFI EventsManager database backend without processing.
Process the logs with the rules selected below before archiving.	Specify the rules to perform before archiving events in GFI EventsManager database backend.
Archive all scanned events in folder storage.	Archives collected events into GFI EventsManager storage folder. For more information on how to configure the storage folder, refer to Configure storage folder section in this manual.

7. Select **Settings** tab and configure the options described in Table 17 below.

Table 17 - Microsoft SQL Database group - Settings

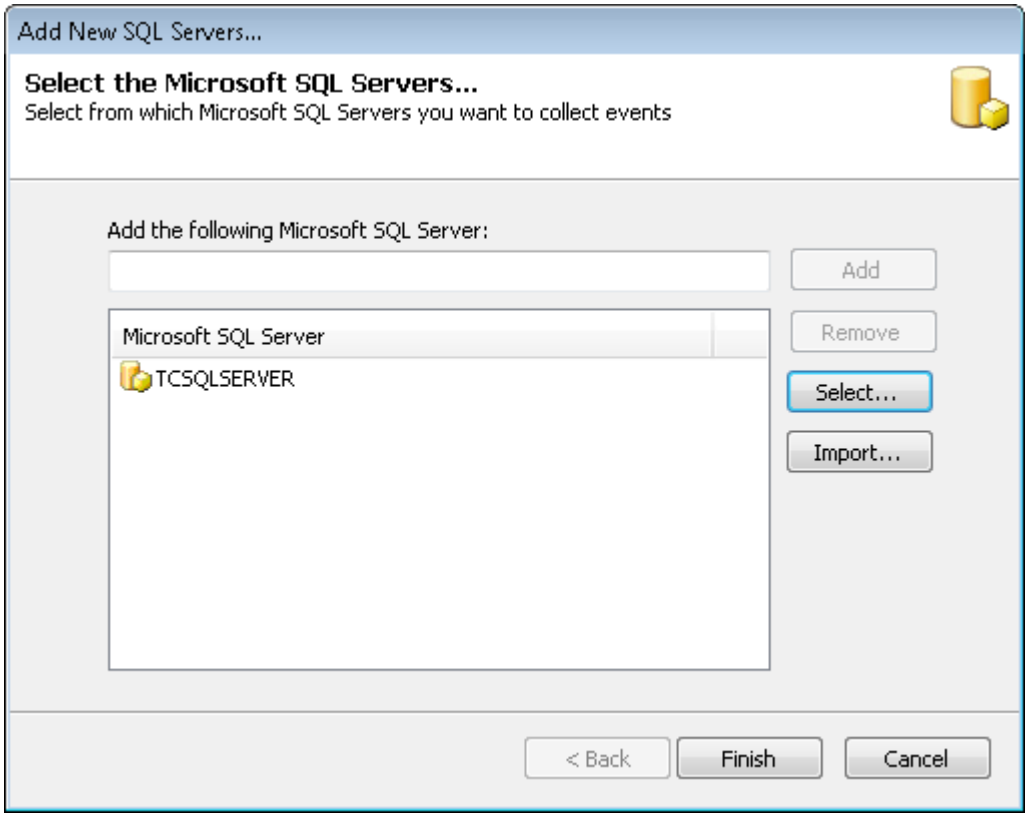
OPTION	DESCRIPTION
Scan all the events for all databases	All Microsoft SQL Server events are collected and processed by GFI EventsManager.
Scan only security events for all databases	Only security events are collected and processed by GFI EventsManager.

8. Click **OK**

6.5.2 Adding a new Microsoft SQL Server

To add a new Microsoft SQL Database to a database group:

1. Right-click the database group and select **Add new SQL Server**.

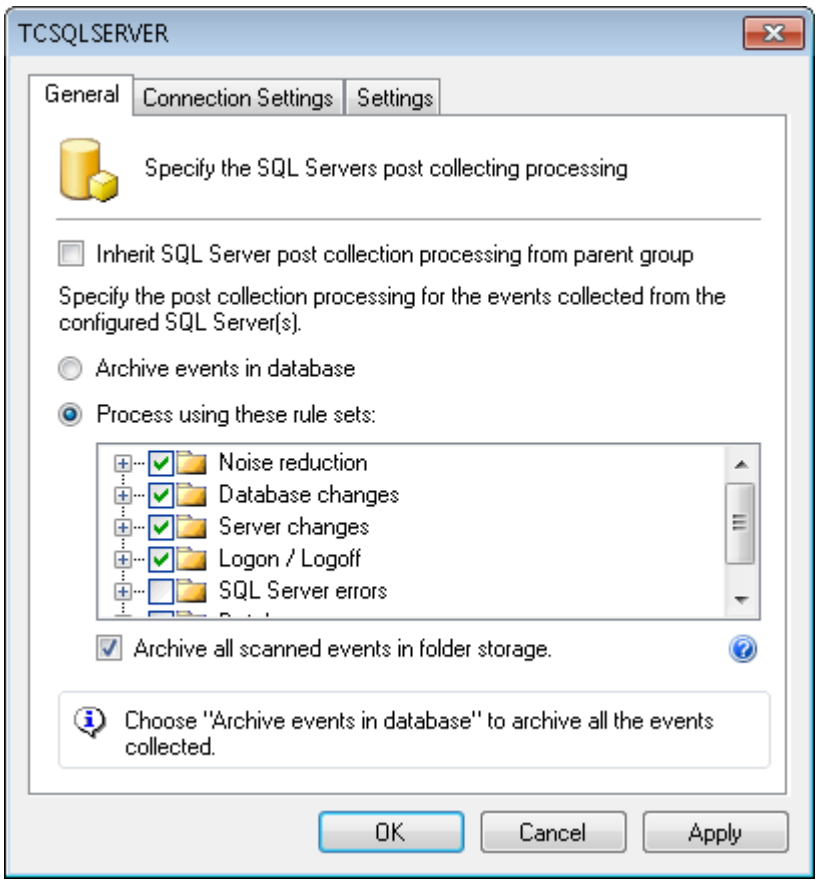


Screenshot 69 - Add new Microsoft SQL server

2. Key-in the server name or IP and click **Add**.

Use **Select** and **Import** to search the network for SQL Servers or import list of SQL servers from a text file respectively. Click **Finish** when ready.

3. From the left panel, double click the Microsoft SQL Database instance to configure.

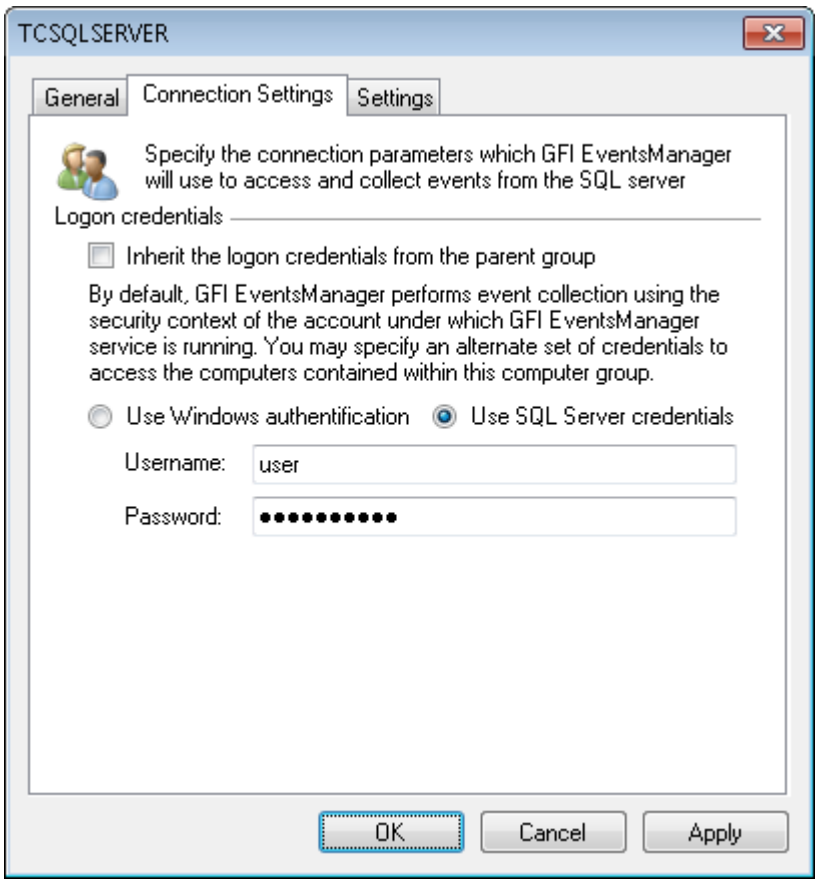

TCSQLSERVER
General
Connection Settings
Settings
Specify the SQL Servers post collecting processing
Inherit SQL Server post collection processing from parent group
Specify the post collection processing for the events collected from the configured SQL Server(s).
Archive events in database
Process using these rule sets:
Noise reduction
Database changes
Server changes
Logon / Logoff
SQL Server errors
Archive all scanned events in folder storage.
Choose "Archive events in database" to archive all the events collected.
OK
Cancel
Apply

Screenshot 70 - Microsoft SQL Database - General tab

4. In the General tab, configure the options described in Table 18 below.

Table 18 - Microsoft SQL Database - General tab options

OPTION	DESCRIPTION
Inherit SQL Server post collecting processing from parent group.	Inherits all settings from the parent group.
Archive events in database	Archive all events in GFI EventsManager database backend without processing.
Process using these rule sets	Archive all events using the specified rules. Select the rules to apply.
Archive all scanned events in folder storage.	Archives collected events into GFI EventsManager storage folder. For more information on how to configure the storage folder, refer to Configure storage folder section in this manual.

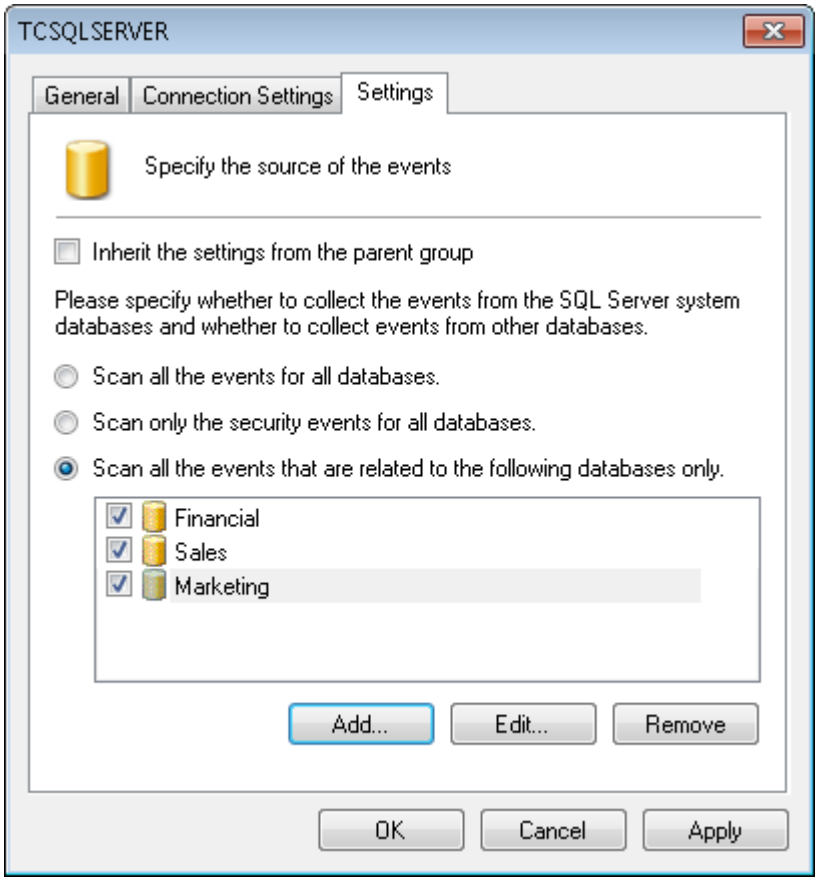

TCSQLSERVER
General
Connection Settings
Settings
Specify the connection parameters which GFI EventsManager will use to access and collect events from the SQL server
Logon credentials
Inherit the logon credentials from the parent group
By default, GFI EventsManager performs event collection using the security context of the account under which GFI EventsManager service is running. You may specify an alternate set of credentials to access the computers contained within this computer group.
Use Windows authentification
Use SQL Server credentials
Username:
user
Password:
OK
Cancel
Apply

Screenshot 71 - Microsoft SQL Database - Connection Settings tab

5. Select **Connection Settings** and configure the options described in Table 19 below.

Table 19 - Microsoft SQL Database - Connection Settings tab

OPTION	DESCRIPTION
Inherit the logon credentials from the parent group	Select this option to inherit login settings from the parent group.
Use Windows authentication	Connect to Microsoft SQL Database using windows authentication.
Use SQL Server credentials	Connect to Microsoft SQL Database using a Microsoft SQL Database user account. Key in a username and password.



Screenshot 72 - Microsoft SQL Database - Settings tab

6. Select **Settings** tab and configure the options described in Table 20 below.

Table 20 - Microsoft SQL Database - Settings tab options

OPTION	DESCRIPTION
Inherit the settings from the parent group	Inherits settings from the parent group.
Scan all the events for all databases	Scan all databases and collect all events from the Microsoft SQL Server.
Scan only the security events for all databases	Scan all databases and collect only security events from the Microsoft SQL Server.
Scan all the events that are related to the following databases only.	Collect all events from the selected databases. Use **Add**, **Edit** and **Remove** to manage database sources.

7. Click **OK**.

6.6 Oracle Server sources

6.6.1 Introduction

GFI EventsManager enables you to collect and process events generated by Oracle Relational database management systems. The following audits are collected and processed by GFI EventsManager:

- **Session auditing** - Audit user sessions and database access.
- **Statements auditing** - Audit SQL statements.
- **Object auditing** - Audit queries and statements related to specific objects.

The following Oracle Database versions are supported:

» Oracle Database 9i
» Oracle Database 10g
» Oracle Database 11g

6.6.2 Pre-configuration settings for Oracle servers

Step 1 - Before collecting events from Oracle servers ensure that the account used to connect, set audits and access the audit table has the necessary permissions.

Step 2 - Enable auditing on the Oracle server by changing startup parameters. To enable auditing:

1. Startup parameters for the Oracle servers are stored in <*Oracle Home Directory*>*admin*\<*Oracle SID*>*pfile**init.ora* file.

2. Locate and open the parameters file using a text editor.

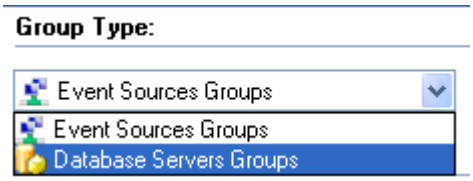
3. Locate AUDIT_TRAIL parameter and change the default value to 'db' or 'db_extended' ('db,extended' on latest versions of Oracle).

4. Save and restart the Oracle server.

6.6.3 Adding a new Oracle Database group

To add a new Oracle Database group:

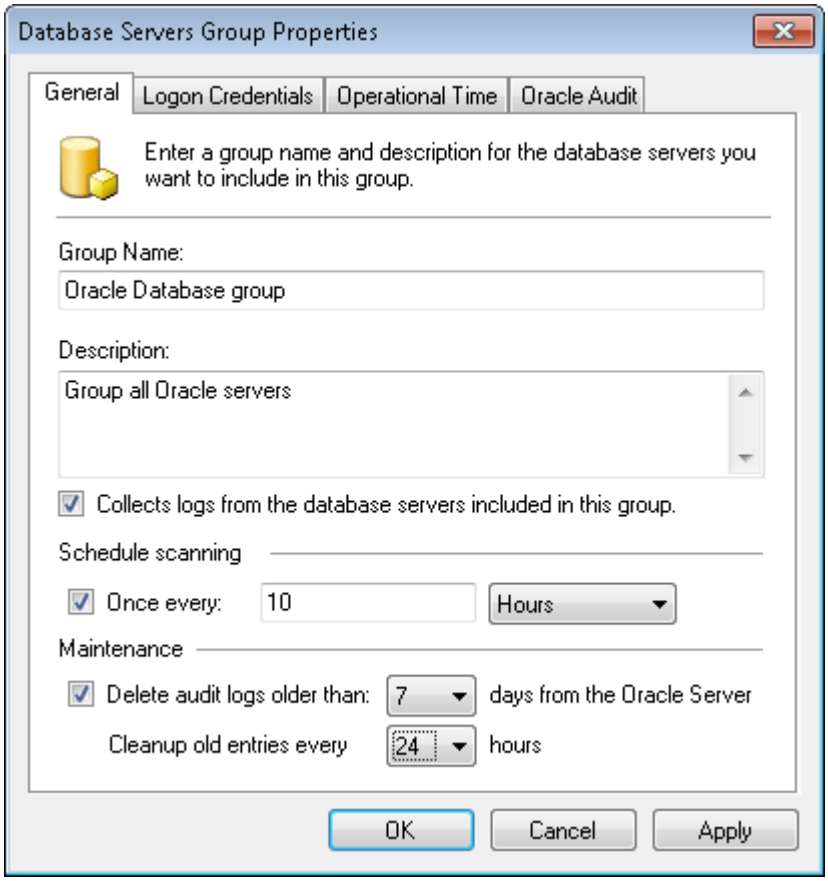
1. Click **Configuration** ► **Event Sources** and from the **Group Type**, select **Database Servers Groups**.



Screenshot 73 - Database Servers Groups

2. From the right panel, right click **Oracle Servers** and select **Create group…**

3. Select **Oracle Server** as the server type.



Screenshot 74 - Oracle Database group - General tab

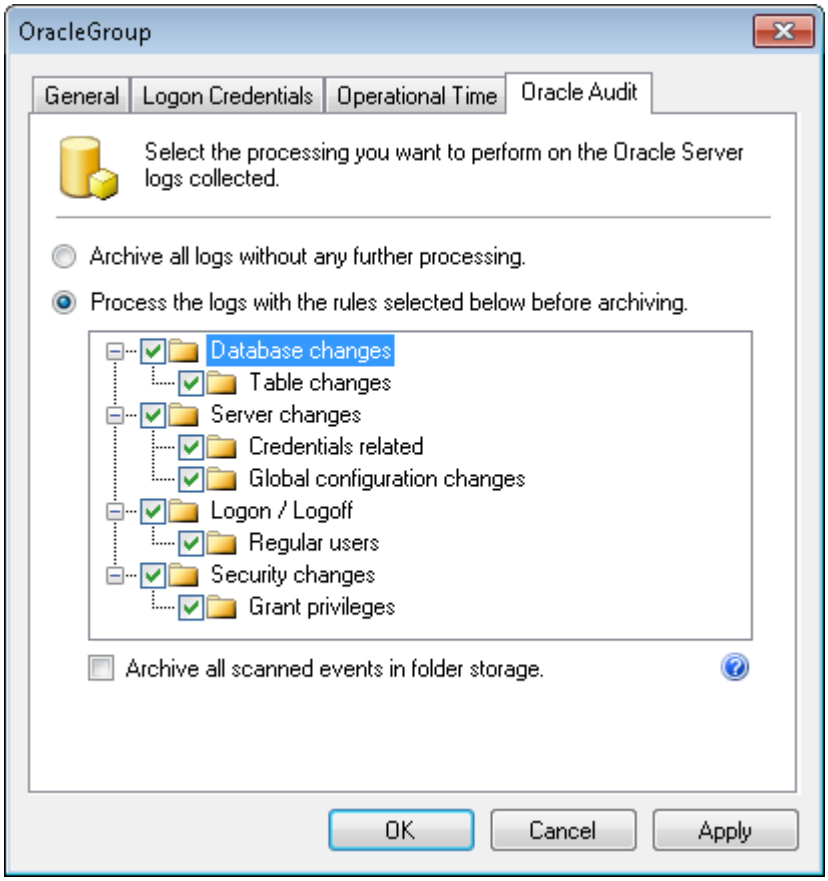
4. In the General tab, configure the options described in Table 21 below.

Table 21 - Oracle Database group - General tab

OPTION	DESCRIPTION
Group Name	Key in a group name to identify the Oracle Database group.
Description	Optional, key-in a description.
Collects logs from the database servers included in this group.	Collects events from the event sources in the Oracle group. Once this option is enabled, configure the **Schedule scanning** and **Maintenance** options.
Schedule scanning	Select **Once every** and configure frequency to collect events on a pre-defined schedule.
Maintenance	Oracle audit events are stored in a specific audit table on the Oracle server. To prevent excessive audit table growth, configure the options in this section to delete audit logs and old entries on a pre-defined time.

5. Select **Logon Credentials** tab and key-in a valid username and password to connect to the Oracle server.

6. Select **Operational Time** tab and configure the normal operational time of the Oracle Database servers in this group.



Screenshot 75 - Oracle Database group - Oracle Audit tab

7. Select **Oracle Audit** and configure the options described in Table 22 below.

Table 22 - Oracle Database group - Oracle Audit

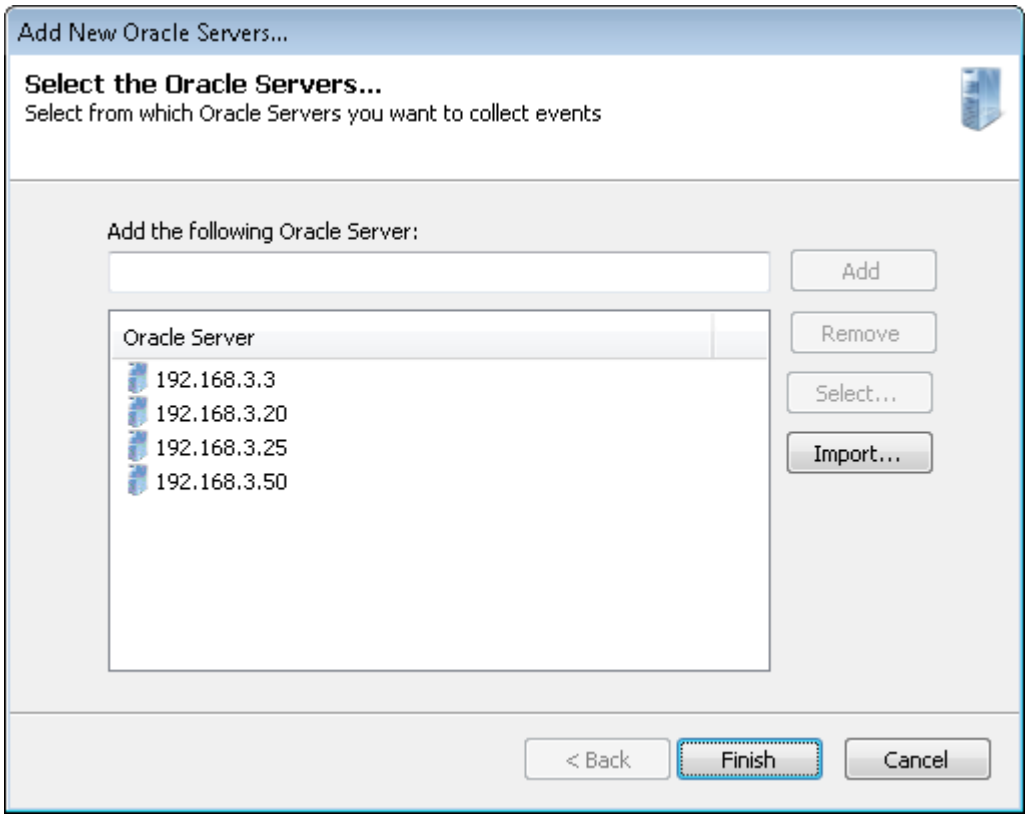
OPTION	DESCRIPTION
Archive all logs without further processing	Enable to archive events in the database backend without processing.
Process the logs with the rules selected below before archiving.	Select option to specify the rules to perform before archiving events in the database backend.
Archive all scanned events in folder storage.	Enable to archive collected events to folder storage. For more information on how to configure folders storage, refer to Configure storage folder section in this manual.

8. Click **OK**

6.6.4 Adding a new Oracle Database

To add a new Oracle Database to a database group:

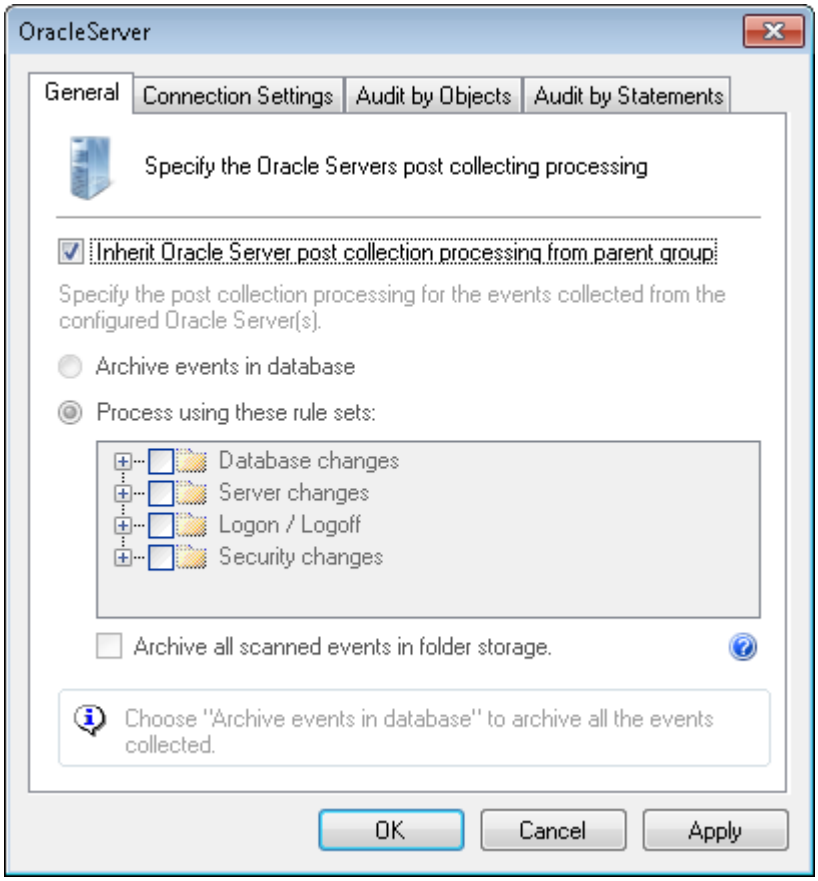
1. Right click the database group and select **Add new Oracle Server**.



Screenshot 76 - Add new Oracle server

2. Key-in the server name or IP and click **Add**. To import the server list from a text file, click **Import** and locate the text file.

3. From the left panel, double click the Oracle Database instance to configure the database options for.

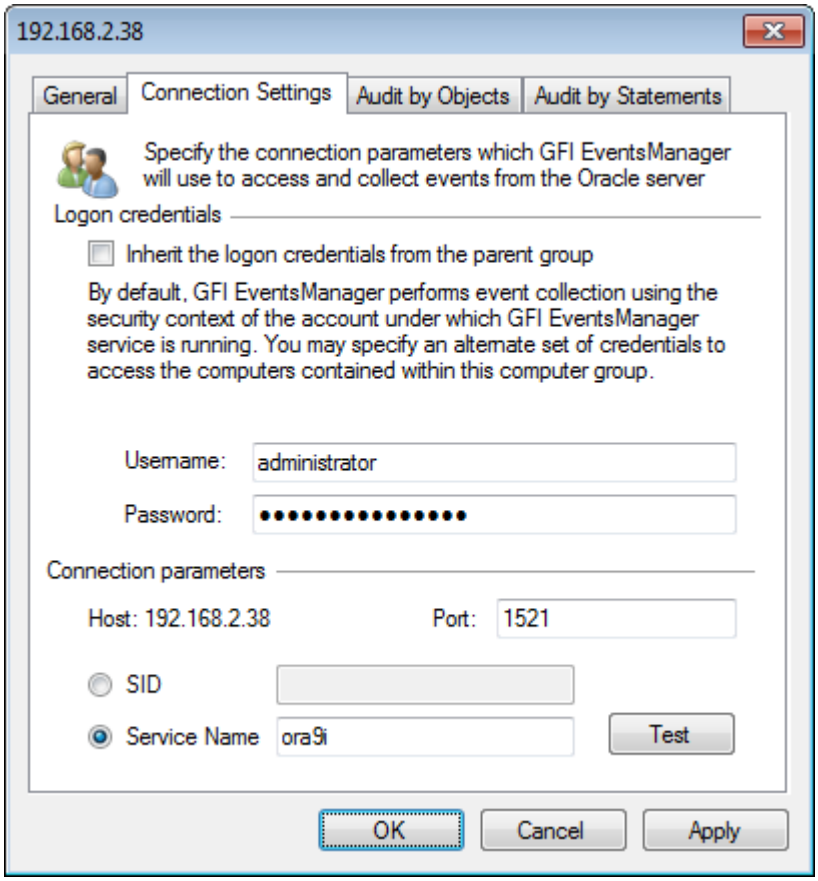

OracleServer
General
Connection Settings
Audit by Objects
Audit by Statements
Specify the Oracle Servers post collecting processing
Inherit Oracle Server post collection processing from parent group
Specify the post collection processing for the events collected from the configured Oracle Server(s).
Archive events in database
Process using these rule sets:
Database changes
Server changes
Logon / Logoff
Security changes
Archive all scanned events in folder storage.
Choose "Archive events in database" to archive all the events collected.
OK
Cancel
Apply

Screenshot 77 - Oracle Database - General tab

4. Configure the options described in Table 23 below.

Table 23 - Oracle Database - General tab options

OPTION	DESCRIPTION
Inherit Oracle Server post collecting processing from parent group.	Select to inherit all settings from the parent group.
Archive events in database	Archive all events in the database backend without processing.
Process using these rule sets	Archive all events using the specified rules. Select the rules to apply.
Archive all scanned events in folder storage.	Select option to archive collected events into the folder storage. For more information on how to configure folders storage, refer to Configure storage folder section in this manual.

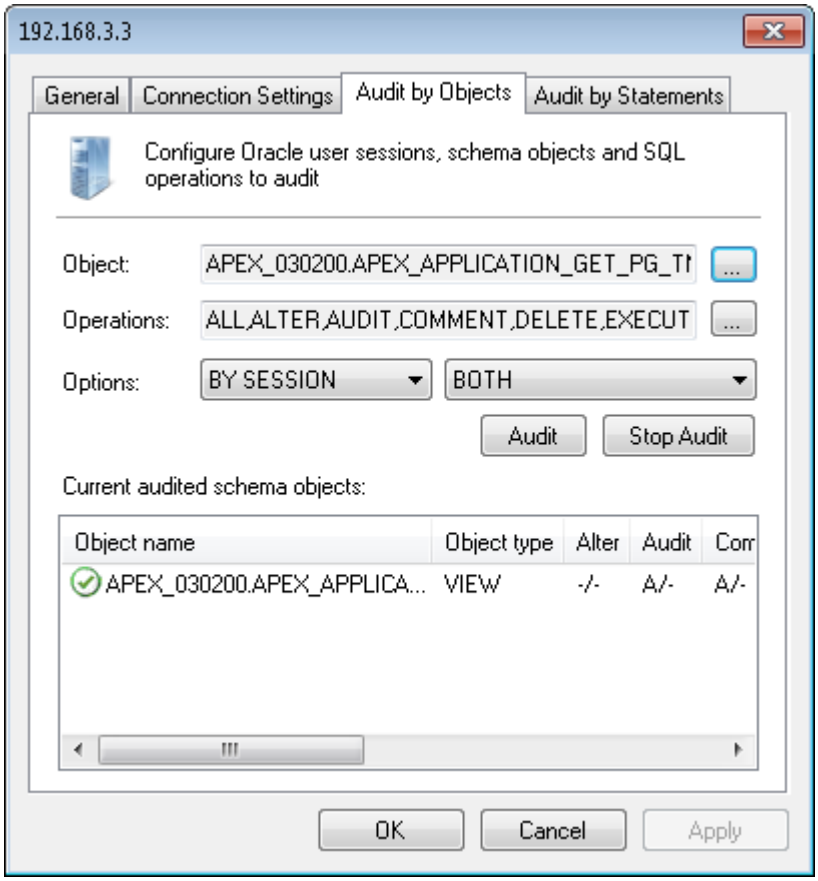

192.168.2.38
General
Connection Settings
Audit by Objects
Audit by Statements
Specify the connection parameters which GFI EventsManager will use to access and collect events from the Oracle server
Logon credentials
Inherit the logon credentials from the parent group
By default, GFI EventsManager performs event collection using the security context of the account under which GFI EventsManager service is running. You may specify an alternate set of credentials to access the computers contained within this computer group.
Username:
administrator
Password:
Connection parameters
Host: 192.168.2.38
Port:
1521
SID
Service Name
ora9i
Test
OK
Cancel
Apply

Screenshot 78 - Oracle Database - Connection Settings tab

5. Select **Connection Settings** and configure the options described in Table 24 below

Table 24 - Oracle Database - General tab options

OPTION	DESCRIPTION
Inherit the logon credentials from the parent group	Select to inherit login settings from the parent group.
Port	Key in the port to use to connect to the Oracle Database.
SID	The SID is a unique name to identify an Oracle Database instance. Key in the SID of the database to audit.
Service Name	The Service name is the alias used to identify the Oracle Database. Key in the Service name of the database to audit.
Test	Test the connection with the Oracle Database server.

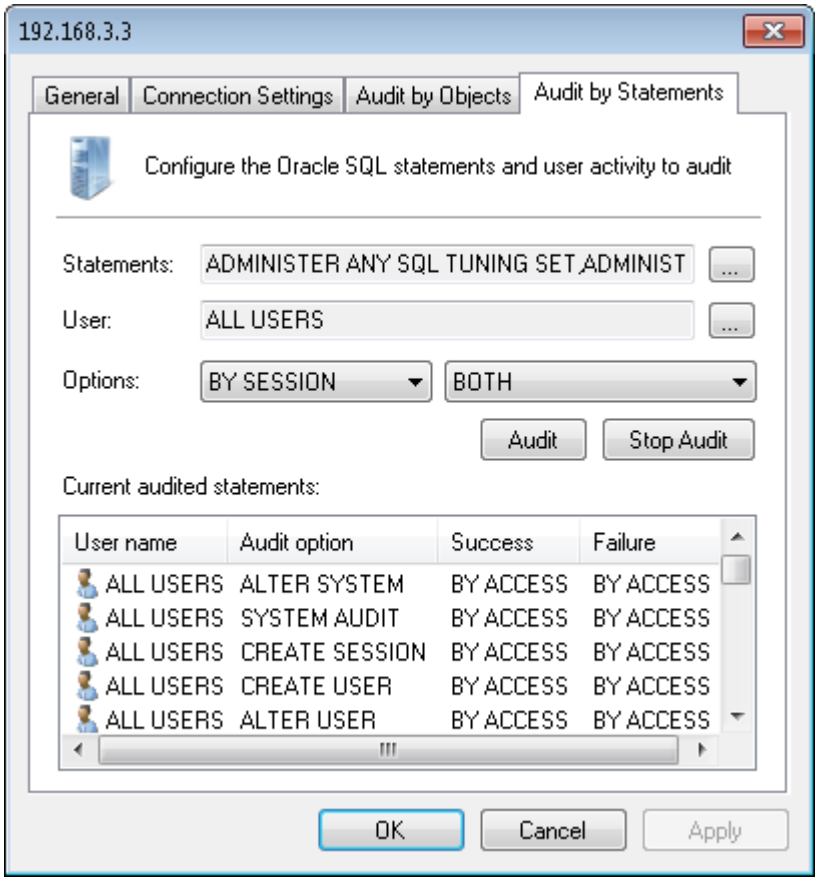


Screenshot 79 - Oracle Database -Audit by objects tab

6. Select **Audit by Objects** and configure the options described in Table 25 below.

Table 25 - Oracle Database - Audit by Objects

OPTION	DESCRIPTION
Object	Click **Browse** to launch a list of available Oracle SQL objects. Select the object to audit and click **OK**. **NOTE**: Amongst others, Oracle objects can be procedures, views, functions and tables.
Operations	Operations are actions that modify or query an object. Click **Browse** to launch a list of available operations. Select the operations to audit and click **OK**.
Options	Select the audit options: » **By Access** - Creates an audit log per object operation execution. » **By Session** - Creates an audit log per operation and per schema object. A session is the time between a connection and a disconnection to/from the database. » **Success** - Select to process only successful audits. » **Failure** - Select to process only failed audits. Oracle will create an audit log if an audit fails to complete. » **Both** - Select to process all audit logs.
Audit	Choose this option to instruct the Oracle server to start auditing the server activities corresponding to the selected parameters (like users, statements, etc.)
Stop Audit	Choose this option to instruct the Oracle server to stop auditing the server activities corresponding to the selected parameters (like users, statements, etc.)
Current audited schema objects	A list that displays all current Oracle audited schema.



Screenshot 80 - Oracle Database -Audit by statements tab

7. Select **Audit by Statements** and configure the options described in Table 26 below.

Table 26 - Oracle Database - Audit by Statements

OPTION	DESCRIPTION
Statements	Click browse button to launch a list of available SQL statements. Select the SQL statements to audit and click **OK**. **NOTE**: Amongst others, Oracle statements can be ALTER, CREATE and SELECT SQL statements.
User	Oracle enables you to audit statements for a specific user. Click browse button to launch a list of available users. Select the user and click **OK**.
Options	Select audit options: » **By Access** - Creates one audit log for each statement execution. » **By Session** - Creates one audit log per user and per schema object. A session is the time between a connection and a disconnection to/from the database. » **Success** - Processes only successful audits. » **Failure** - Select option to process only failed audits. Oracle will create an audit log if an audit fails to complete. » **Both** - Select option to process all audit logs.
Audit	Choose this option to instruct the Oracle server to start auditing the server activities corresponding to the selected parameters (like users, statements, etc.)
Stop Audit	Choose this option to instruct the Oracle server to stop auditing the server activities corresponding to the selected parameters (like users, statements, etc.)
Current audited statements	A list that displays all current Oracle audited statements.

8. Click **OK**.

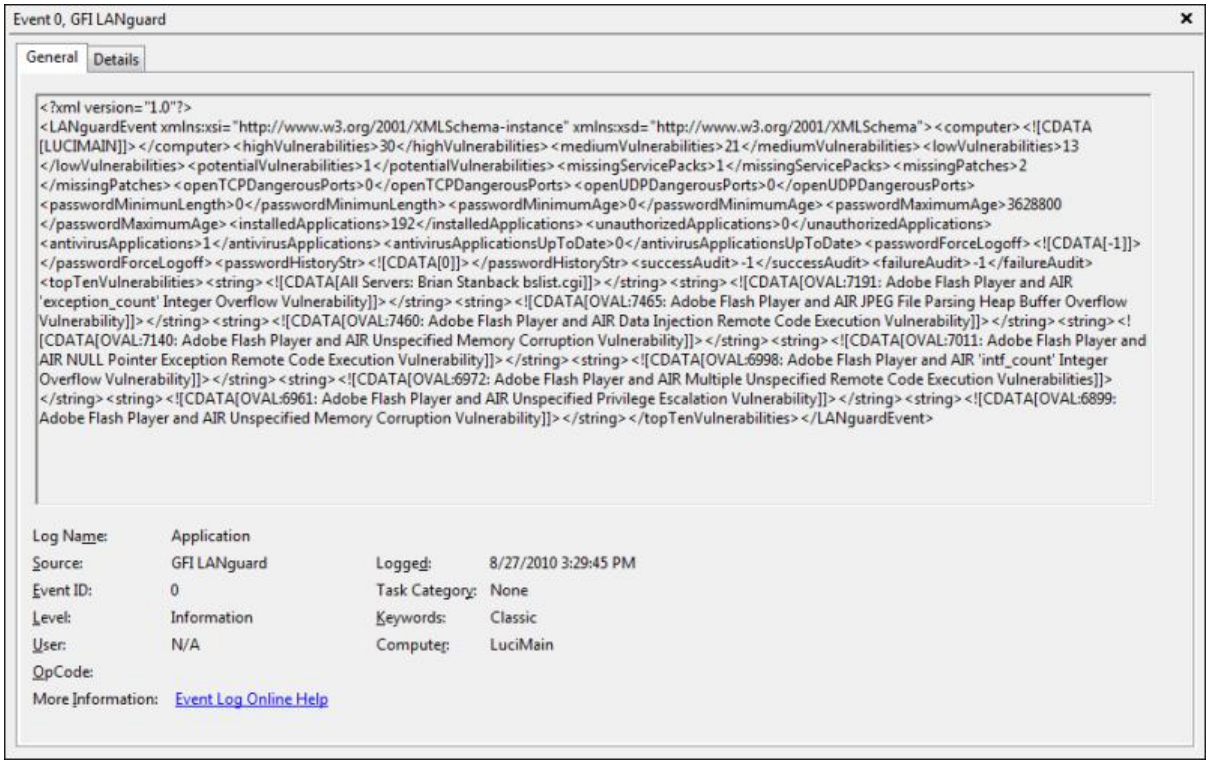
6.7 Adding GFI LANguard event sources

6.7.1 Introduction

GFI EventsManager enables you to monitor events generated by GFI LANguard. GFI LANguard is a network vulnerability scanner that audits your network for weaknesses that can be exploited by users for malicious purposes. During network audits, GFI LANguard creates events in the 'Application Log' of the machine where it is installed/running.

For each machine scanned by GFI LANguard, an 'Application log' entry having 'Event ID: 0' and 'Source' set as GFI LANguard will be generated. These events denote network vulnerability information extracted from scanned computers including:

» Threat level
» Missing patches and service packs
» Open ports
» Antivirus operational and malware definition status
» Applications detected on scanned targets



Screenshot 81 - Event generated by GFI LANguard

GFI EventsManager can process events generated by GFI LANguard version 9.5 or later.

6.7.2 How to enable GFI LANguard event logging?

To start monitoring 'Application log' entries generated by GFI LANguard, you must configure GFI EventsManager to scan the Application log of GFI LANguard. This is achieved by adding the machine where GFI LANguard is installed to the list of event sources in GFI EventsManager. For information on how to manage event sources, refer to Manage event sources chapter in this manual.

Once GFI LANguard machine is added as an event source, GFI EventsManager will remotely and automatically enable the event logging feature in GFI LANguard by creating and setting the following registry value on the GFI LANguard machine:

```
HKEY_LOCAL_MACHINE\SOFTWARE\GFI\LNSS[n]\Config\EventLog = 1 (dword)
```

`[n]` is the major version number of GFI LANguard. For example, for GFI LANguard 9.5, the registry entry would be:
`HKEY_LOCAL_MACHINE\SOFTWARE\GFI\LNSS9\Config\EventLog = 1 (dword)`

To stop GFI LANguard from generating 'Application Log' entries, remove the registry value described above or change the registry value to 0.

6.7.3 Monitor GFI LANguard Events

GFI EventsManager has built-in processing rules for GFI LANguard events that are enabled by default. To monitor events generated by GFI LANguard, select **Status** tab ► **General** and locate the **Critical and High Importance Events** section.

Vulnerability/threats are grouped by type (for example Vulnerabilities, missing patches, missing service packs)

To configure GFI LANguard event processing rules, click **Configuration** tab ► **Event Processing Rules** and from the left pane select **GFI Rules** ► **GFI LANguard rules**. For more information on event processing rules, refer to Using event processing rules chapter in this manual.

6.8 Adding GFI EndPointSecurity event sources

6.8.1 Introduction

GFI EndPointSecurity enables you to maintain data integrity by preventing unauthorized access and transfer of content to and from the following devices or connection ports:

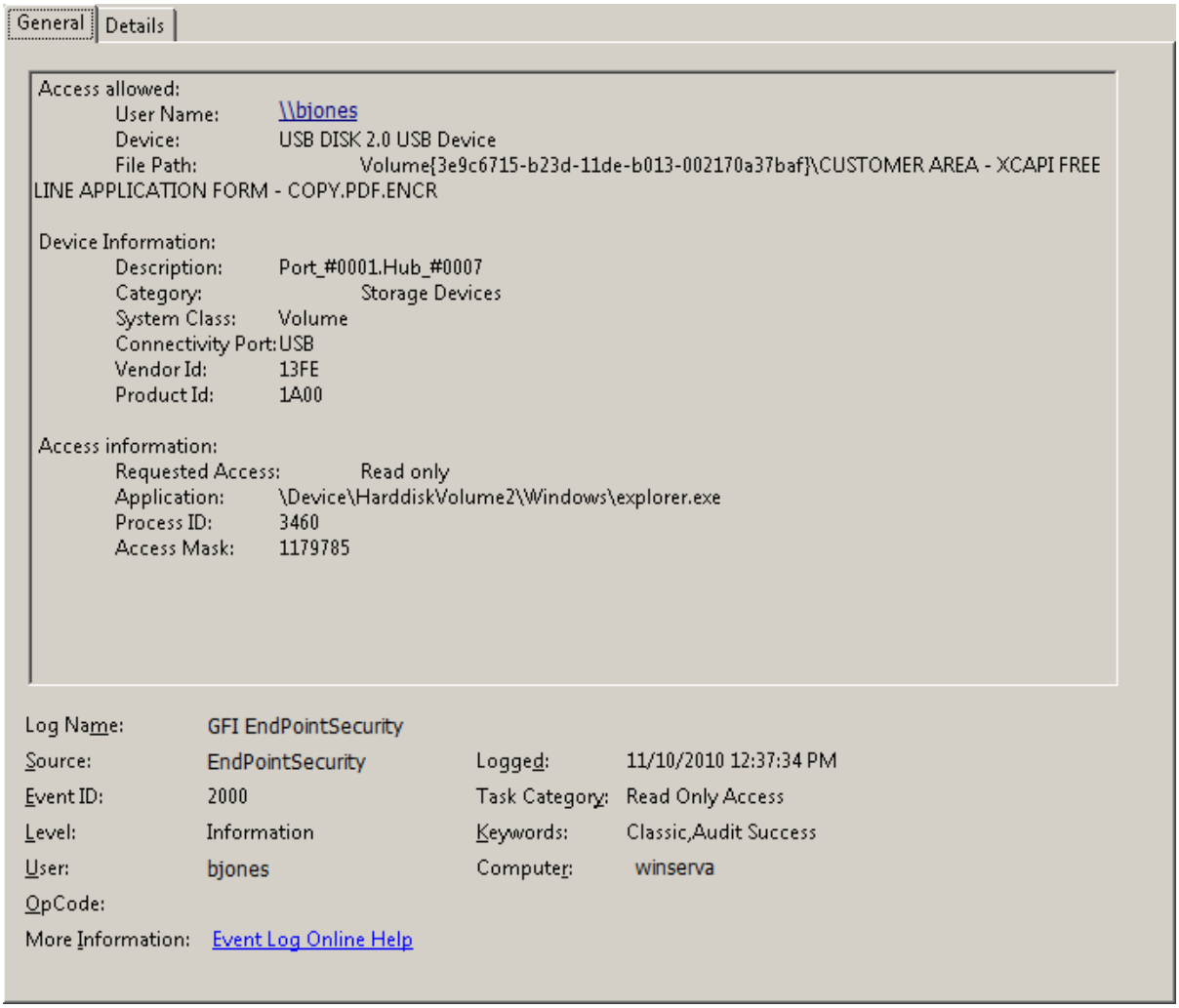
- USB Ports (e.g. Flash and Memory card readers, pen drives)
- Firewire ports (e.g. digital cameras, Firewire card readers)
- Wireless data connections (e.g. Bluetooth and Infrared dongles)
- Floppy disk drives (internal and external)
- Optical drives (e.g. CD, DVD)
- Magneto Optical drives (internal and external)
- Removable USB hard-disk drives
- Other drives such as Zip drives and tape drives (internal and external).

For more information on GFI EndPointSecurity, refer to http://www.gfi.com/endpointsecurity

6.8.2 Enable GFI EndPointSecurity logging

By default GFI EndPointSecurity is configured to generate log events with information on:

- The GFI EndPointSecurity service
- Devices connected and disconnected on your network
- Access allowed or denied by GFI EndPointSecurity to users.



Screenshot 82 - Event generated by GFI EndPointSecurity

To configure the logging options in GFI EndPointSecurity:

1. From the GFI EndPointSecurity machine, launch GFI EndPointSecurity management console.

2. Click **Configuration** tab ► **Protection Policies**.

3. From the left pane, select the protection policy and click **Set Logging Options**.

4. Customize the settings available in **Logging Option** dialog.

For more information on how to configure GFI EndPointSecurity logging options, refer to the GFI EndPointSecurity documentation available from http://www.gfi.com/products/gfi-endpointsecurity/manual.

6.8.3 Monitor GFI EndPointSecurity Events

GFI EventsManager has built-in processing rules for GFI EndPointSecurity events that are enabled by default. To monitor events generated by GFI EndPointSecurity, select **Status** tab ► **General** and locate the **Critical and High Importance Events** section.

To configure GFI EndPointSecurity event processing rules, click **Configuration** tab ► **Event Processing Rules**. From the left pane, select **GFI Rules** ► **GFI EndPointSecurity rules**. For more information on event processing rules, refer to Using event processing rules chapter in this manual.

7 Using event processing rules

7.1 Introduction

GFI EventsManager allows you to collect and process: Windows Event Logs, W3C logs, Syslogs, SNMP Traps and Microsoft SQL Server audit logs. All supported log types record events in a different and proprietary format; therefore every log type requires different configuration settings and parameters. You can configure log collection and processing parameters:

- On a computer by computer basis
- On a computer group by computer group basis.

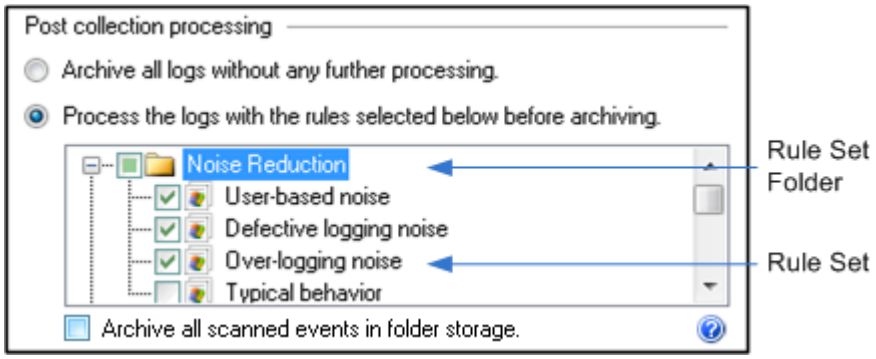
During event processing, GFI EventsManager runs a configurable set of rules against the collected logs in order to classify events and trigger alerts/actions accordingly. By default, GFI EventsManager ships with a pre-configured set of event processing rules that allow you to gain network-wide control over computer logs - with negligible configuration effort.

Event processing rules

Event processing rules are instructions/checks that:

- Analyze the collected logs.
- Classify the severity of processed events. Classification is based on the configuration settings of the processing rule.
- Filter events that match specific criteria. For example, you can create and run a rule which filters out low severity events and noise (duplicate events).
- Generate alerts and actions based on event severity. For example, you can configure GFI EventsManager to send both SMS and Email alerts whenever an event is classified as critical; but limit the product to send only email alerts when an event is classified as high in severity. For more information on how to configure alerts and actions refer to Configuring alerting options section in this manual.
- Optionally archive filtered events. Event archiving is based on the severity of the event and on the configuration settings of the event processing rules. For example, you can configure GFI EventsManager to archive only events that are classified critical or high in severity and discard all the rest.

In GFI EventsManager, event processing rules are organized into 'Rule-sets'; and every rule-set can contain one or more specialized rules which can be run against collected logs.



Screenshot 83 - Rule-sets folder and Rule-sets

Rule-sets are further organized into **Rule-sets Folders**. This way you can group rule-sets according to the functions and actions that the respective rules perform. By default, GFI EventsManager ships with pre-configured folders, rule-sets and event processing rules that can be further customized to suite your event processing requirements.

Event classification

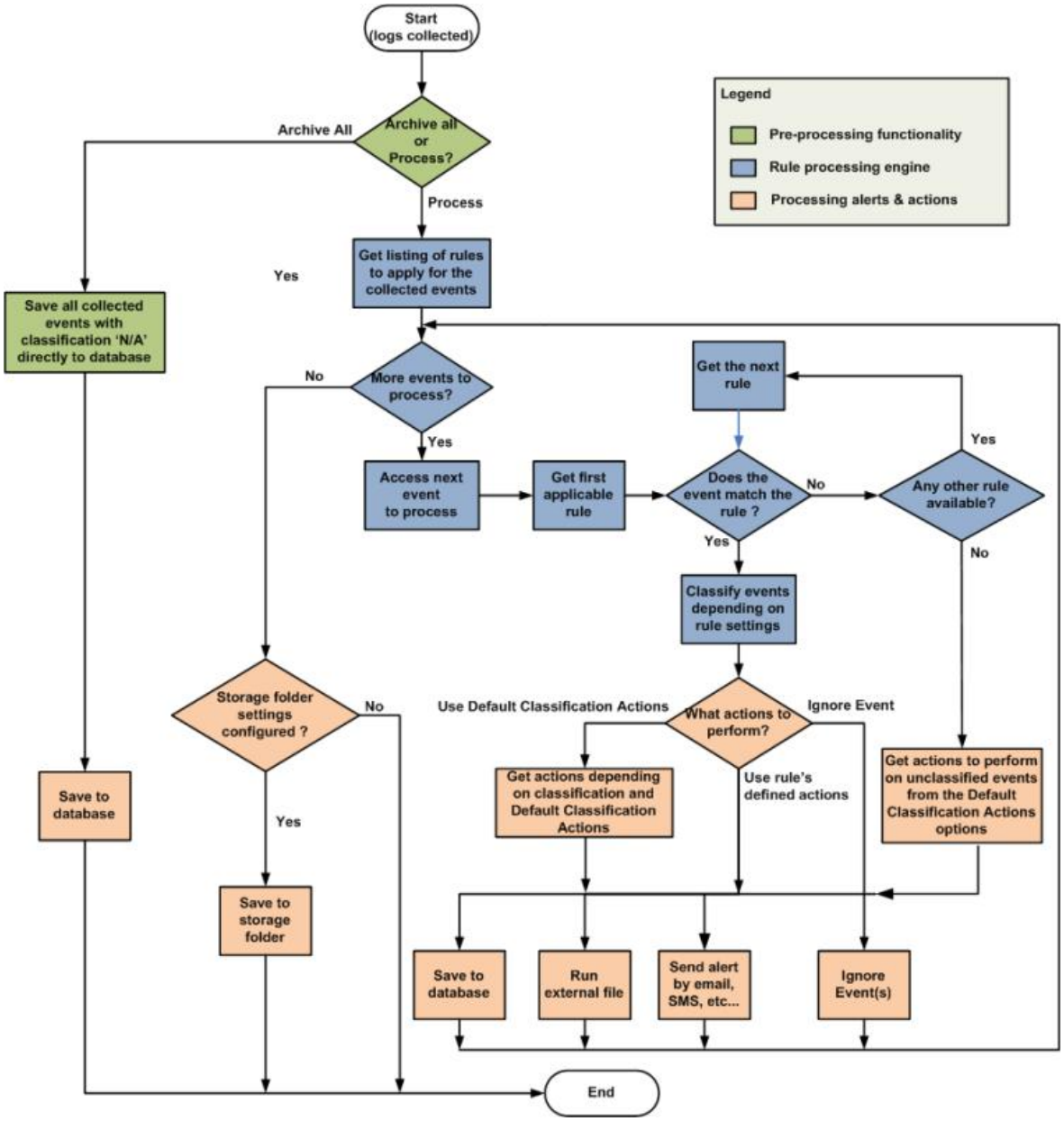
GFI EventsManager classifies events in 5 categories:

- Critical
- High
- Medium
- Low
- Noise (unwanted or repeated log entries).

Event classification is based on the configuration of the rules that are executed against the collected logs. Events that don't satisfy any event classification conditions are tagged as unclassified and can be set to trigger the same alerts and actions available for classified events.

7.2 How event processing works

The flowchart chart below illustrates the event processing stages performed by GFI EventsManager.

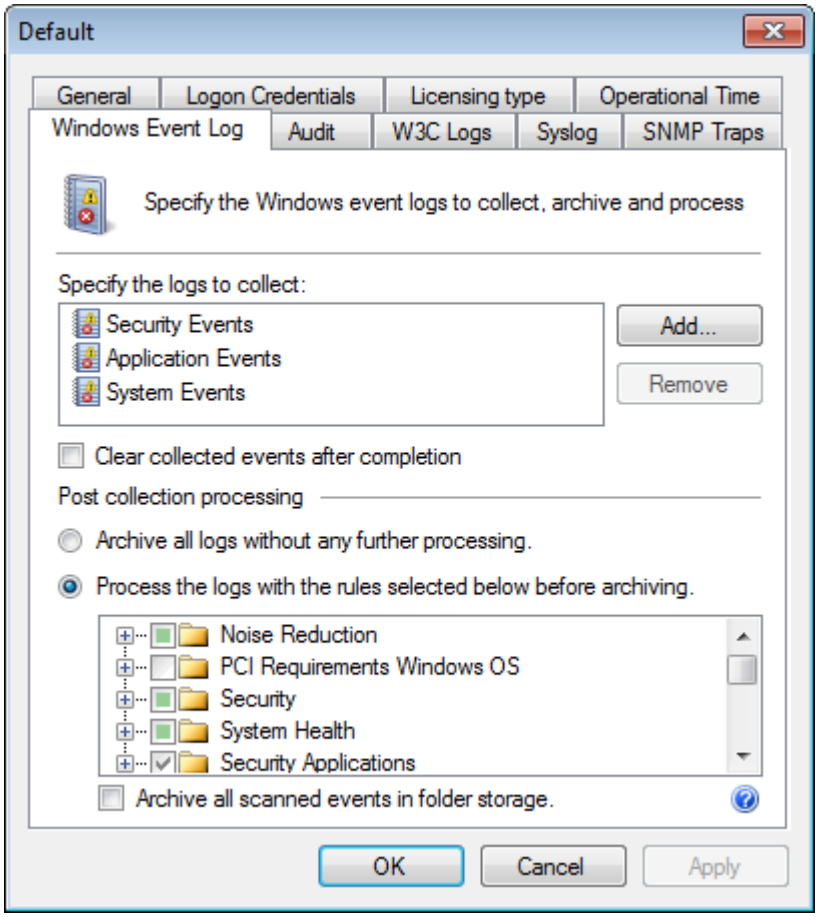


Screenshot 84 - Log processing, classification and actions flowchart

7.3 Collecting events

7.3.1 Collecting Windows events

Windows events are organized into specific log categories; by default computers running on Windows NT or higher record errors, warnings and information events in 3 logs namely Security, Application and System logs. Computers that have more specialized roles on the network (For example: Domain Controllers, DNS Servers, ET cetera.) have additional event log categories.

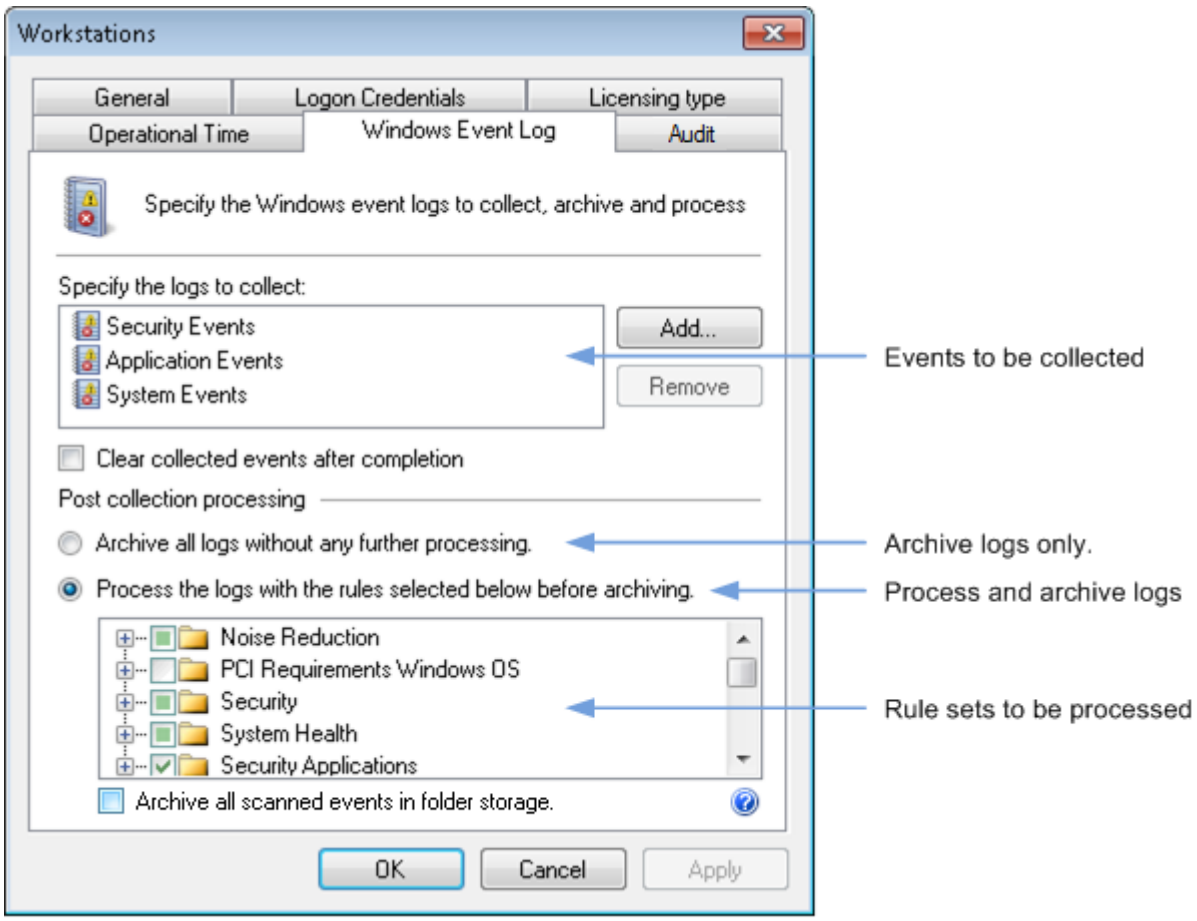


Screenshot 85 - Computer group properties: Configuring logs to be processed

As a minimum, Windows Operating Systems record events in the following logs:

- **Security event log:** This log contains security related events through which you can audit successful or attempted security breaches. Typical events found in the Security Events log include valid and invalid logon attempts.
- **Application event log:** This log contains events recorded by software applications/programs such as file errors.
- **System event log:** This log contains events logged by operating system components such as failures to load device drivers.
- **Directory service log:** This log contains events generated by the Active Directory including successful or failed attempts to make to update the Active Directory database.
- **File Replication service log:** This log contains events recorded by the Windows File Replication service. These including file replication failures and events that occur while domain controllers are being updated with information about sysvol.
- **DNS server log:** This log contains events associated with the process of resolving DNS names to IP addresses.

» **Application and Services Logs:** These logs contain events associated with Windows VISTA and the relative services/functionalities it offers.



Screenshot 86 - Computer group properties: Configuring Windows Event Logs parameters

To configure Windows Event Log collection and processing parameters you must:

» Select the events to be collected.

» Specify whether the collected logs will be processed (filtered, etc.) or just archived without processing.

» Select the event processing rule-sets/rules that will be run against the collected logs.

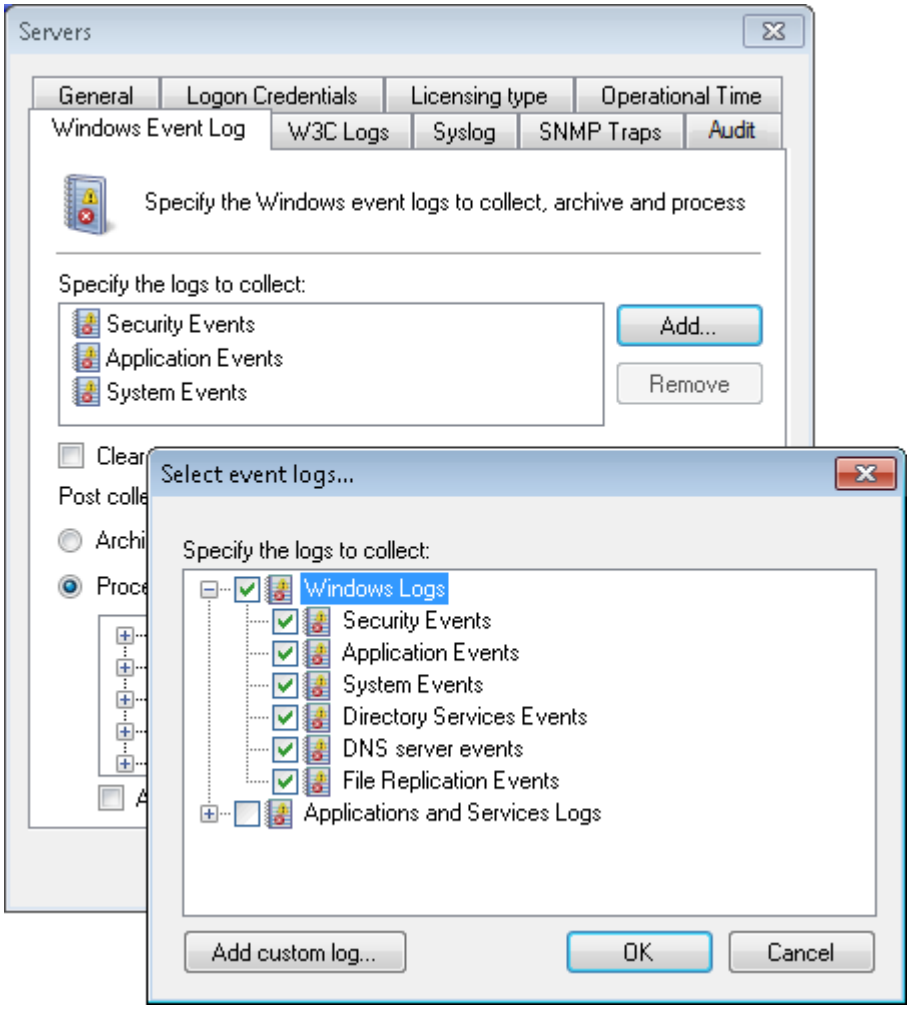
» Select if the events will be stored in the storage folder. For more information on how to archive events in a storage folder, refer to Configure storage folder section in this manual.

Selecting the events to be collected

To specify which Windows events will be collected by GFI EventsManager:

1. Launch the (computer/computer group) properties dialog.

2. Click **Windows Event Log** tab.



Screenshot 87 - Selecting the events to be collected

3. Click **Add** and select the events that will be collected.

GFI EventsManager supports custom event logs. For information on how to configure custom event logs please refer to Collecting custom events section in this chapter.

4. (Optional) Select **Clear collected events after completion** to clear the collected events from event sources.

Deleting Syslog messages without archiving may lead to legal compliance issues.

7.3.2 Collecting W3C logs

W3C is another log format supported by GFI EventsManager. W3C logs are text-based flat files containing various event details delimited by special characters.

The W3C log format is mostly commonly used by hardware systems (e.g. servers and appliances) which have internet specific roles. Microsoft Internet Information Server (IIS) service and Apache web servers for example, can collect web related events (i.e. web logs) in the form of W3C formatted text files.

In GFI EventsManager, the configuration process of W3C log parameters is identical to that performed for Windows event processing, with one exception. Unlike Windows Event Logs, there is no standard which dictates a specific or centralized folder location where W3C log files are stored on disk. Therefore, in order to collect W3C logs, you must specify the complete path to these text-based log files.

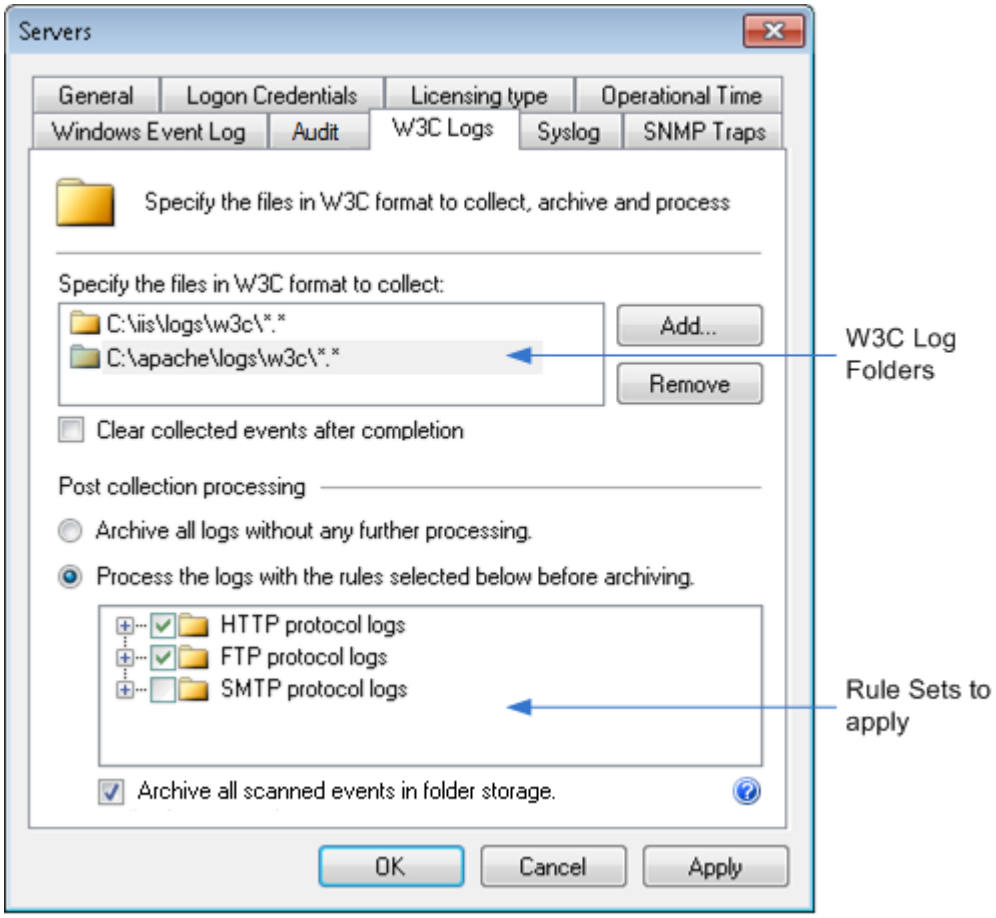
Selecting the events to be collected and processed

To specify which W3C logs will be collected by GFI EventsManager:

1. Click **Configuration** tab ► **Event Sources**

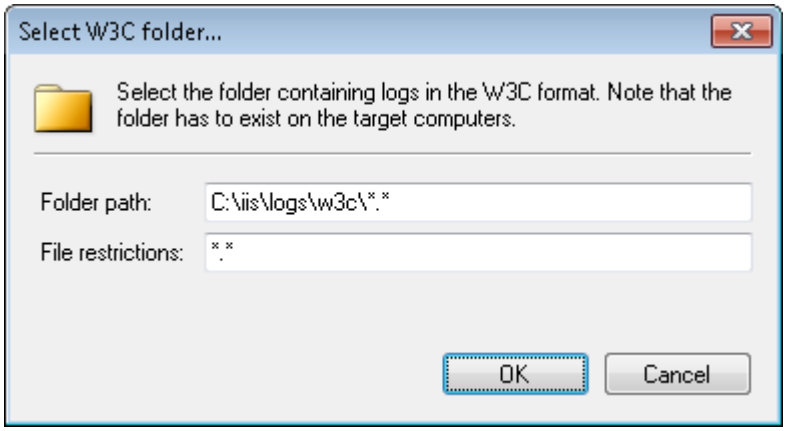
2. Right-click a group or a single computer and select **Properties**.

3. Select **W3C Logs** tab.



Screenshot 88 - Computer group properties: Configuring W3C event processing parameters

4. Click **Add** and specify the log file name and location. Wildcards such as *.* are supported.



Screenshot 89 - Add a new W3C folder path

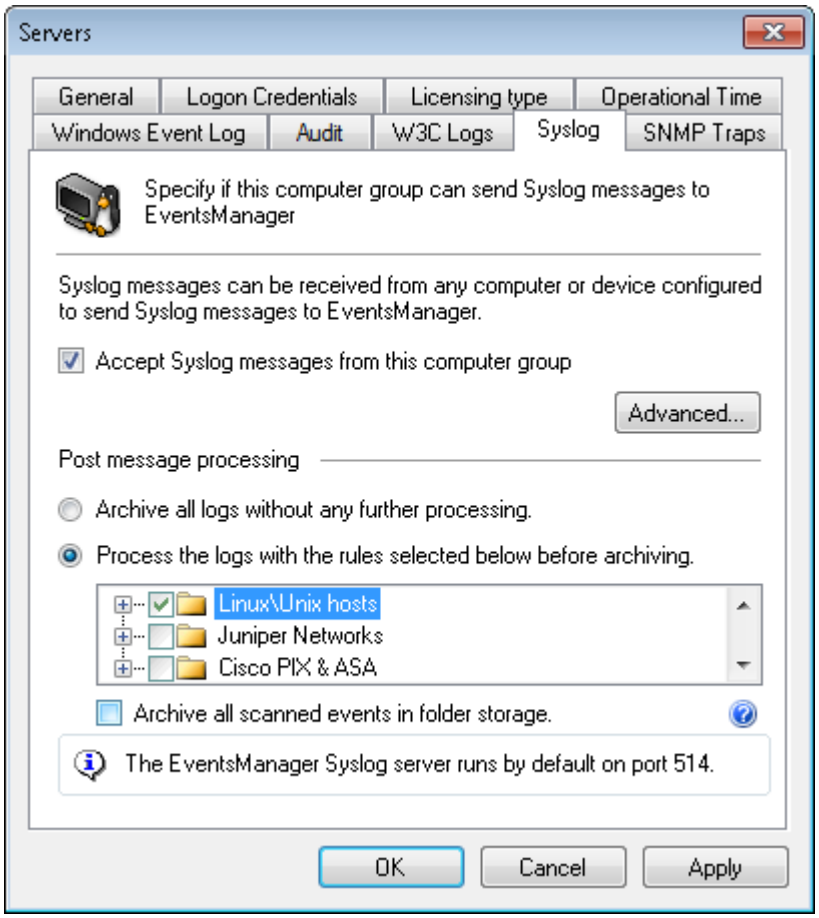
5. (Optional) Select **Clear collected events after completion,** to clear the collected events from event sources.

6. (Optional) Select **Archive all scanned events in folder storage** to archive events in the storage folder after applying the processing rules. For more information on how to configure the storage folder, refer to Configure storage folder section in this manual.

Deleting SNMP messages without archiving may lead to legal compliance issues.

7.3.3 Collecting Syslogs

Syslog is a data logging service that is most commonly used in Linux and UNIX based environments. The concept behind Syslogs is that the logging of events and information is entirely handled by a dedicated server called 'Syslog Server'. This means that unlike Windows and W3C log based environments, regular programs do not log any information. They just send events in the form of data messages (technically known as 'Syslog Messages') to a Syslog server that will manage the message and save the data in a log file.


Servers
General
Logon Credentials
Licensing type
Operational Time
Windows Event Log
Audit
W3C Logs
Syslog
SNMP Traps
Specify if this computer group can send Syslog messages to EventsManager
Syslog messages can be received from any computer or device configured to send Syslog messages to EventsManager.
Accept Syslog messages from this computer group
Advanced...
Post message processing
Archive all logs without any further processing.
Process the logs with the rules selected below before archiving.
Linux\Unix hosts
Juniper Networks
Cisco PIX & ASA
Archive all scanned events in folder storage.
The EventsManager Syslog server runs by default on port 514.
OK
Cancel
Apply

Screenshot 90 - Computer group properties: Syslog processing parameters

In order to process Syslog messages, GFI EventsManager ships with a built-in Syslog Server. This Syslog server will automatically collect, in real-time, all Syslog messages/events sent by Syslog sources and pass them on to the event processing engine. Out-of-the-box GFI EventsManager supports events generated by various network devices manufactured by leading providers including Cisco and Juniper. For more information about supported devices visit:

http://kbase.gfi.com/showarticle.asp?id=KBID002868.

A built-in buffer allows the Syslog server to collect, queue and forward up to 30 Syslog messages for batch processing. Buffered logs are by default passed on to the event processing engine as soon as the buffer fills up or at 1 minute intervals whichever comes first.

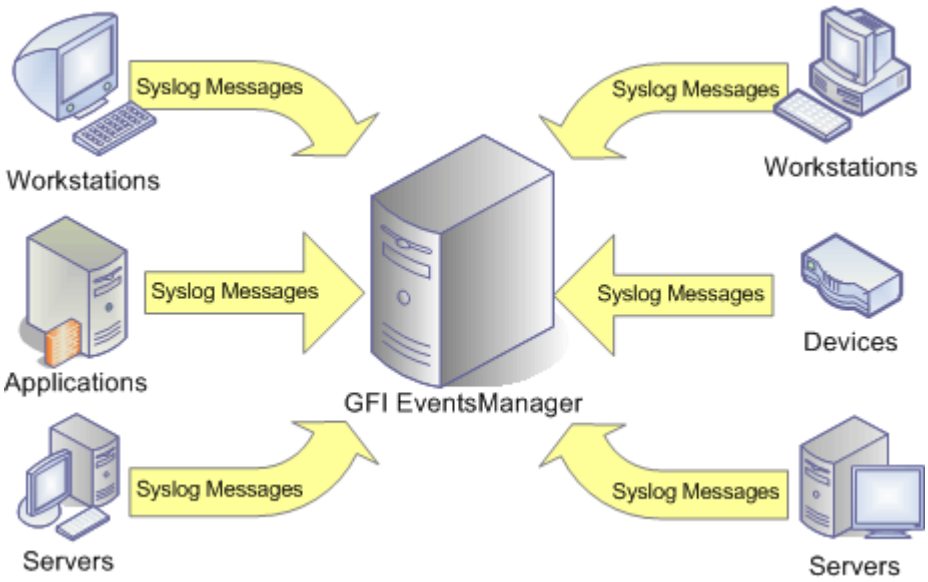


Figure 7 - Syslog messages must be directed to the computer running GFI EventsManager

For Syslog message processing, ALL Syslog sources (e.g. workstations, servers, network appliances, etc.) must be configured to send their messages to the computer/IP where GFI EventsManager is installed. This applies also for the computer that is running GFI EventsManager, in GFI EventsManager, Syslog event processing parameters are configured as follows:

1. Open up the (computer/computer group) properties dialog.

2. Click **Syslog** tab.

3. To enable the Syslog server and listen for messages sent by the computers in a computer group, select **Accept Syslog Messages from this computer group**.

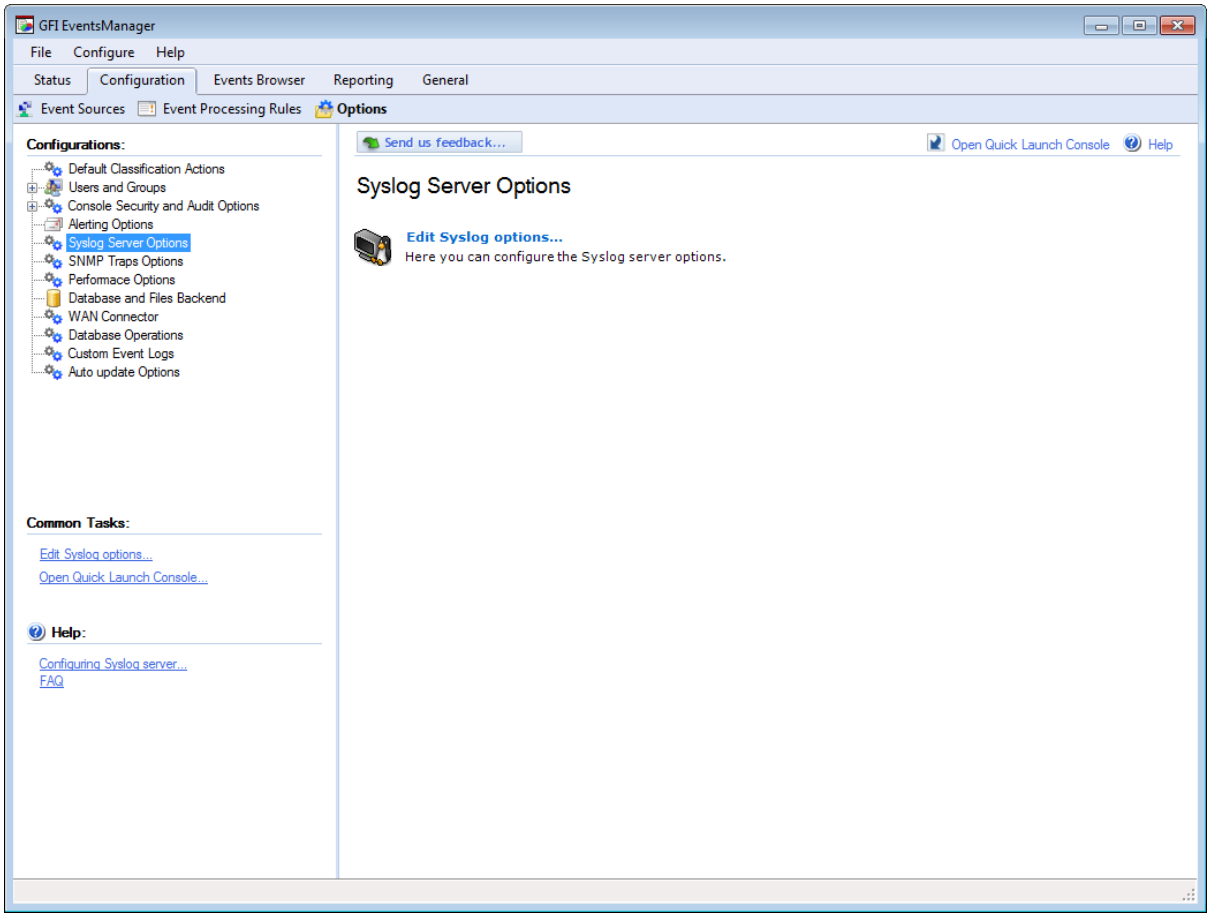
4. Click **Advanced** to enter a custom window code page.

	Windows code page - is used to encode international characters to ASCII strings. Since Syslog is not Unicode compliant, GFI EventsManager uses a code page to decode the events. This is only applicable if GFI EventsManager is installed on a machine using a different language than the monitored machines. For a windows code list , refer to http://www.microsoft.com/globaldev/reference/wincp.mspx

5. (Optional) Select **Archive all scanned events in folder storage**, to archive events in the storage folder. For more information on how to configure the storage folder, refer to Configure storage folder section in this manual.

	Deleting events from source logs without archiving may lead to legal compliance issues.
	The GFI EventsManager Syslog server is by default configured to listen for Syslog messages on port 514. For more information on how to customize Syslog server port settings refer to Configuring the Syslog server communications port section in this chapter.
	The built-in Syslog server will only accept Syslog messages sent from the computers that are part of this computer group.

7.3.4 Configuring the Syslog server communications port



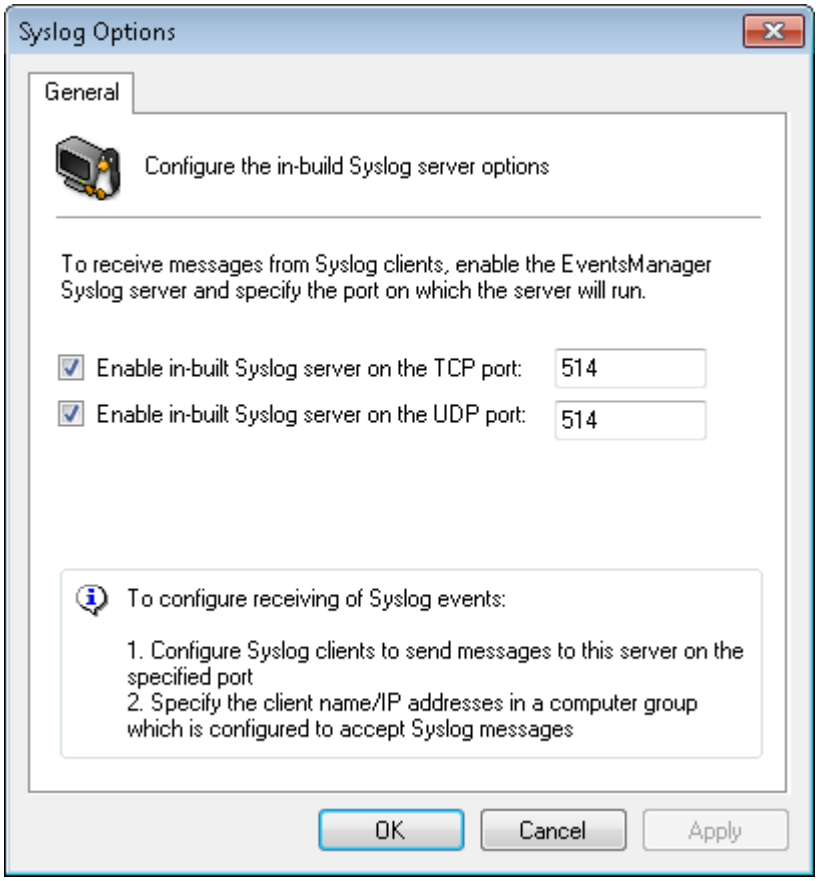
Screenshot 91 - Configuring Syslog Server

To change the default Syslog ports settings:

1. Select **Configuration** tab

2. Select **Options** from the tab options.

3. From the left pane, right-click the **Syslog Server Options** node and select **Edit Syslog options…**


Syslog Options
General
Configure the in-build Syslog server options
To receive messages from Syslog clients, enable the EventsManager Syslog server and specify the port on which the server will run.
Enable in-built Syslog server on the TCP port:
514
Enable in-built Syslog server on the UDP port:
514
To configure receiving of Syslog events:
1. Configure Syslog clients to send messages to this server on the specified port
2. Specify the client name/IP addresses in a computer group which is configured to accept Syslog messages
OK
Cancel
Apply

Screenshot 92- Syslog server properties

4. Select **Enable in-built Syslog server on TCP / UDP port:** and specify the TCP/UDP port on which GFI EventsManager will receive/listen for Syslog messages.

5. Select **OK** to finalize settings.

When configuring Syslog server port settings, make sure that the configured port is not already in use by other installed applications. This may affect the delivery of Syslog messages to GFI EventsManager.

7.3.5 Collecting SNMP Traps

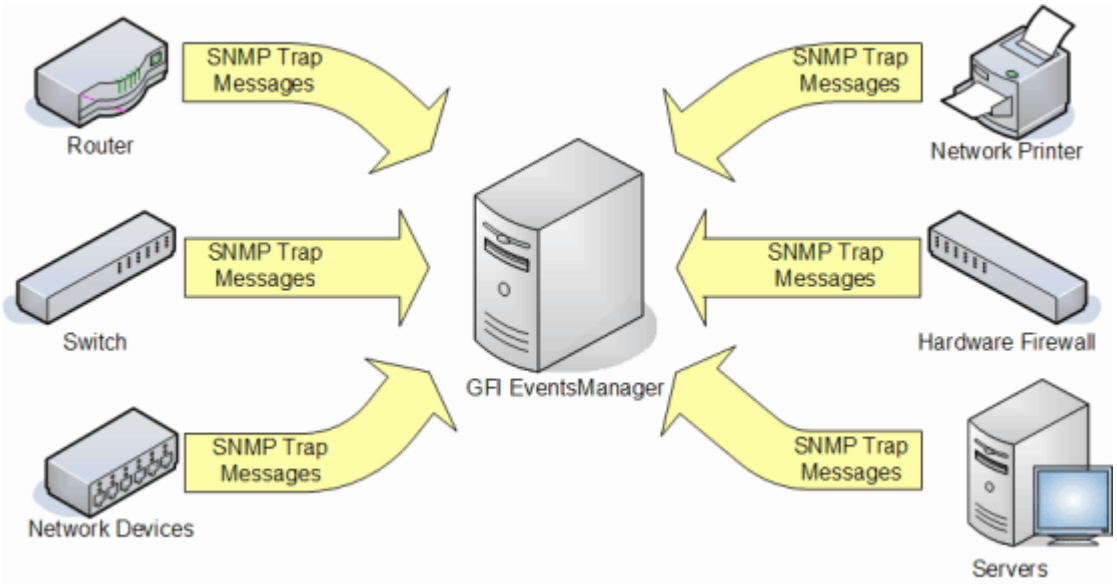
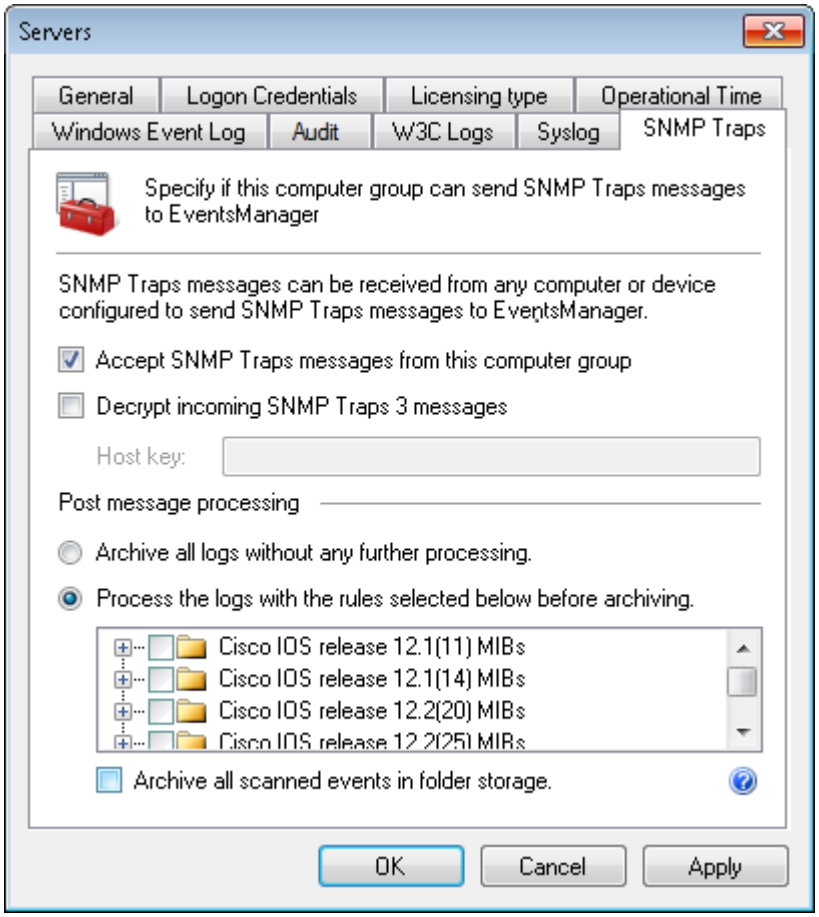


Figure 8: SNMP Trap messages must be directed to the computer running GFI EventsManager

SNMP is a data logging service that enables networked devices to log events and information through data messages (technically known as SNMP Traps). SNMP messaging technology is similar in concept to Syslogs - where unlike Windows and W3C log based

environments, devices that generate SNMP messages do not record events data in local logs. Instead events information is sent in the form of data messages to an SNMP Trap Server which manages and saves SNMP message data in a local (centralized) log file.

GFI EventsManager natively supports an extensive list of SNMP devices and Management Information Bases (MIBs). For a full list of supported devices visit: http://kbase.gfi.com/showarticle.asp?id=KBID002868.


Servers
General
Logon Credentials
Licensing type
Operational Time
Windows Event Log
Audit
W3C Logs
Syslog
SNMP Traps
Specify if this computer group can send SNMP Traps messages to EventsManager
SNMP Traps messages can be received from any computer or device configured to send SNMP Traps messages to EventsManager.
Accept SNMP Traps messages from this computer group
Decrypt incoming SNMP Traps 3 messages
Host key:
Post message processing
Archive all logs without any further processing.
Process the logs with the rules selected below before archiving.
Cisco IOS release 12.1(11) MIBs
Cisco IOS release 12.1(14) MIBs
Cisco IOS release 12.2(20) MIBs
Archive all scanned events in folder storage.
OK
Cancel
Apply

Screenshot 93 - Computer group properties: SNMP processing parameters

GFI EventsManager includes a dedicated SNMP Trap Server through which SNMP Traps are handled. A built-in buffer allows the SNMP Trap Server to collect, queue and forward up to 30 SNMP Trap messages for batch processing. Buffered logs are by default passed on to the event processing engine as soon as the buffer fills up or at 1 minute intervals whichever comes first.

For SNMP Trap processing, ALL sources (e.g. workstations, servers, network appliances, etc.) must be configured to send their messages to the computer/IP where GFI EventsManager is installed. This applies also for the computer that is running GFI EventsManager, to configure SNMP processing parameters

1. Open the computer/computer group properties dialog.

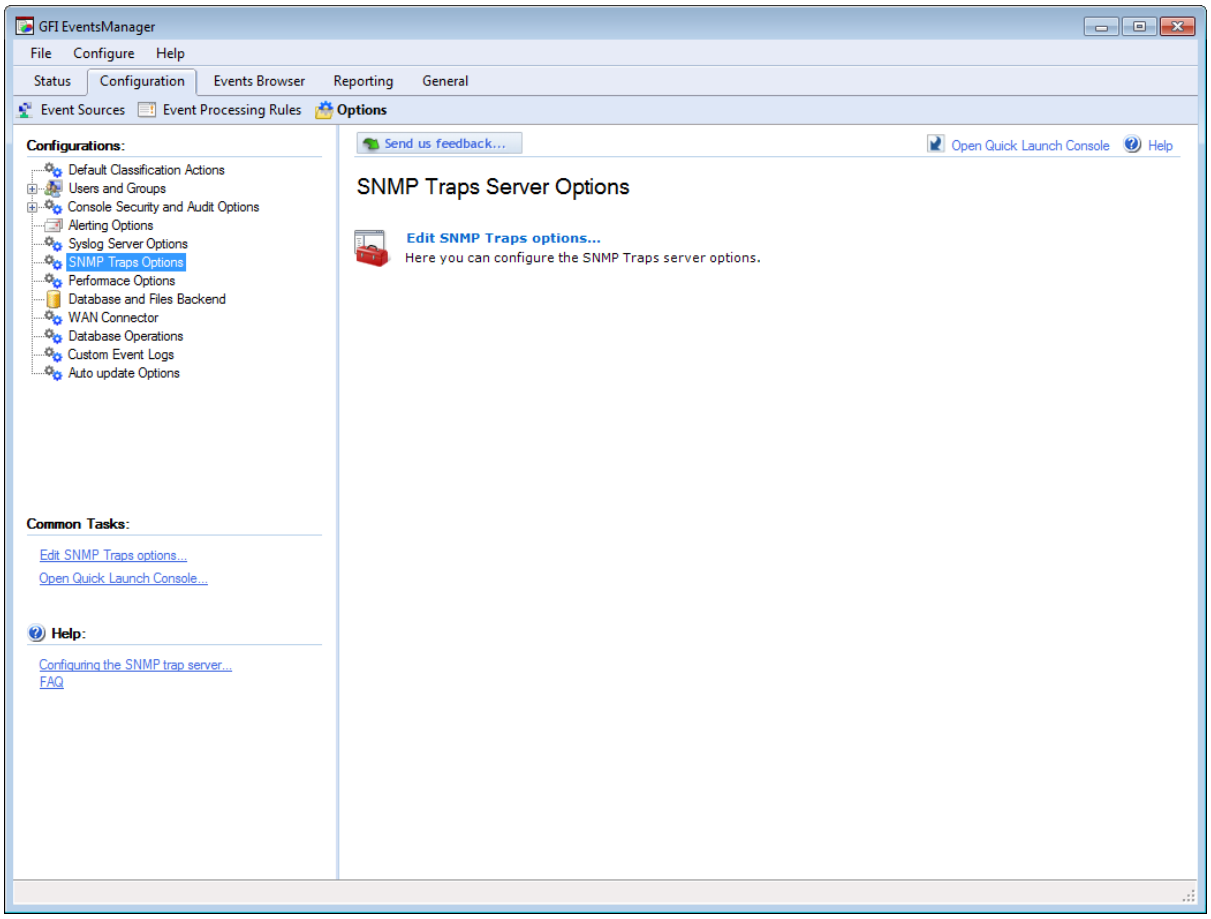
2. Click **SNMP Traps** tab.

3. To listen to SNMP messages via built-in SNMP Trap Server select the **Accept SNMP Traps messages from this computer group**.

	Deleting events from source logs without archiving may lead to legal compliance issues.
	The GFI EventsManager SNMP Trap Server is by default configured to listen for SNMP Trap messages on port 162. For more information on how to customize SNMP Trap Server port settings refer to Configuring the SNMP Trap server settings section in this chapter.

	The built-in SNMP Trap Server will only accept SNMP messages sent from the computers that are part of this computer group.
	The built in SNMP Trap Server supports SNMP version 3 Traps with encryption. For encrypted SNMP messages the encryption host key must be provided in the decrypt incoming SNMP Traps 3 message field

7.3.6 Configuring the SNMP Trap server

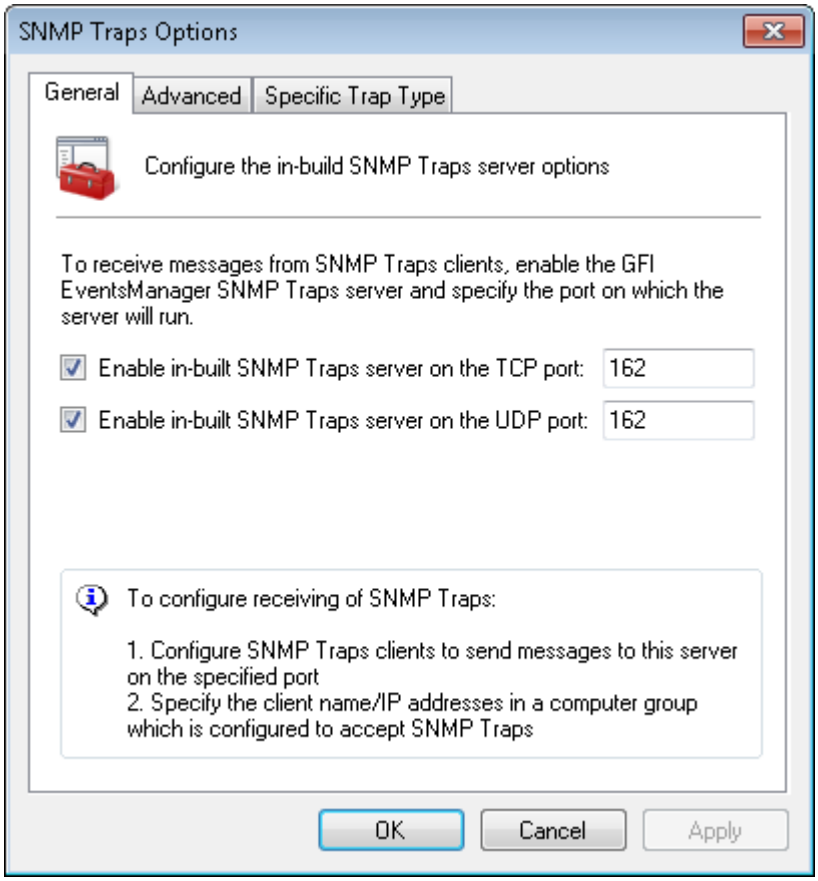


Screenshot 94 - Configuring SNMP Traps

To change the default SNMP Trap Server settings:

1. Click **Configuration** tab and select **Options**.

2. From the left pane, right-click **SNMP Traps Options** node and select **Edit SNMP Traps options…**


SNMP Traps Options
General
Advanced
Specific Trap Type
Configure the in-build SNMP Traps server options
To receive messages from SNMP Traps clients, enable the GFI EventsManager SNMP Traps server and specify the port on which the server will run.
Enable in-built SNMP Traps server on the TCP port:
162
Enable in-built SNMP Traps server on the UDP port:
162
To configure receiving of SNMP Traps:
1. Configure SNMP Traps clients to send messages to this server on the specified port
2. Specify the client name/IP addresses in a computer group which is configured to accept SNMP Traps
OK
Cancel
Apply

Screenshot 95- SNMP Traps options

3. Enable the required TCP/UDP SNMP server. Specify the TCP/UDP port on which GFI EventsManager will listen for SNMP messages.

4. Click **Advanced** tab to add, edit or remove SNMP Trap object identifiers (OIDs).

5. Click **Specific Trap Type** tab to add, edit or remove trap types.

6. Click **OK** to finalize settings.

When configuring SNMP Trap Server port settings, make sure that the configured TCP or UDP port is not already in use by other installed applications. This may affect the delivery of SNMP Trap messages to GFI EventsManager.

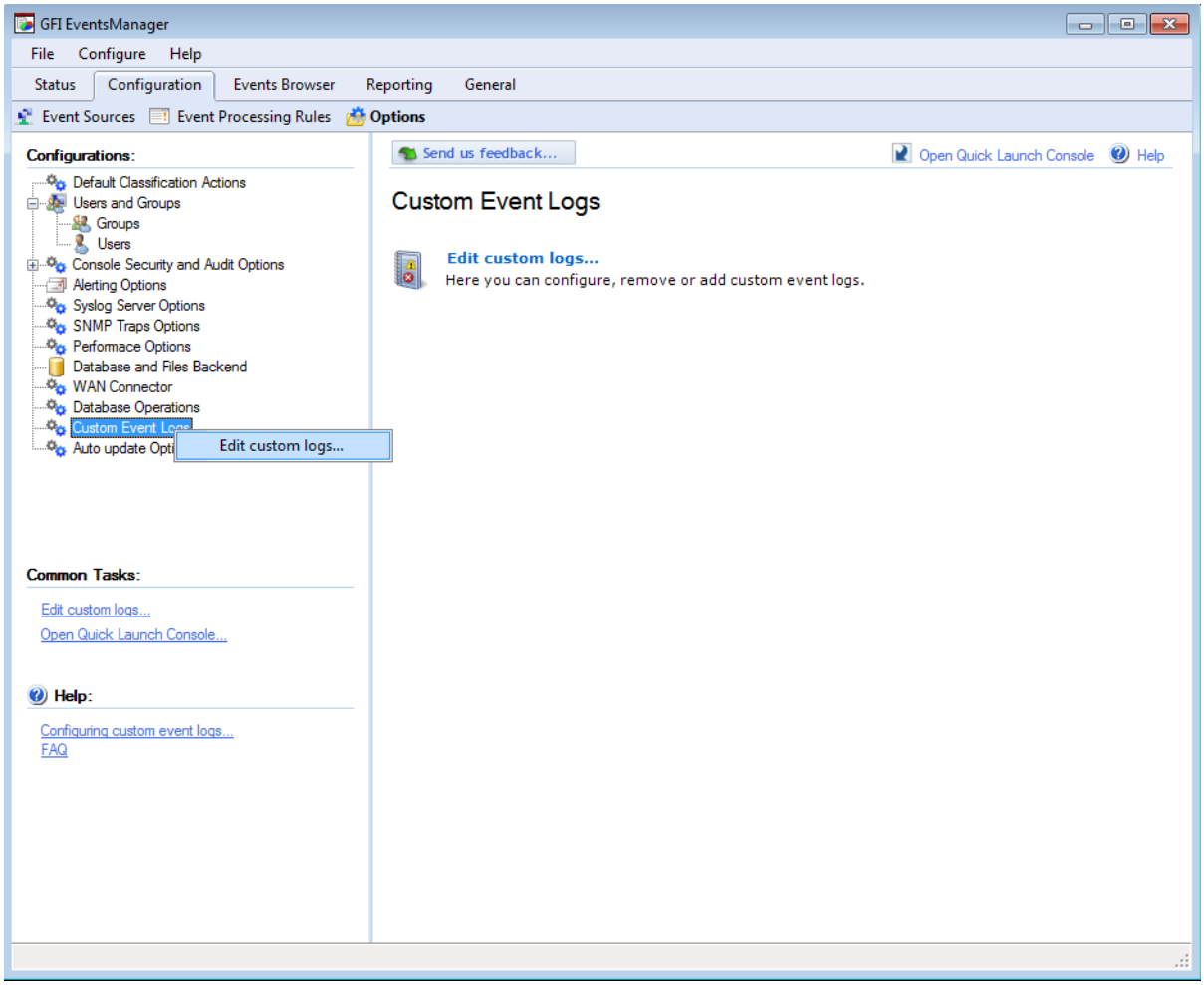
7.3.7 Collecting custom events

GFI EventsManager is configured to collect and process standard Windows Event Logs. However, GFI EventsManager can also be configured to manage events recorded in third party application logs such as anti-virus logs, software firewall logs and other security software.

To configure custom events:

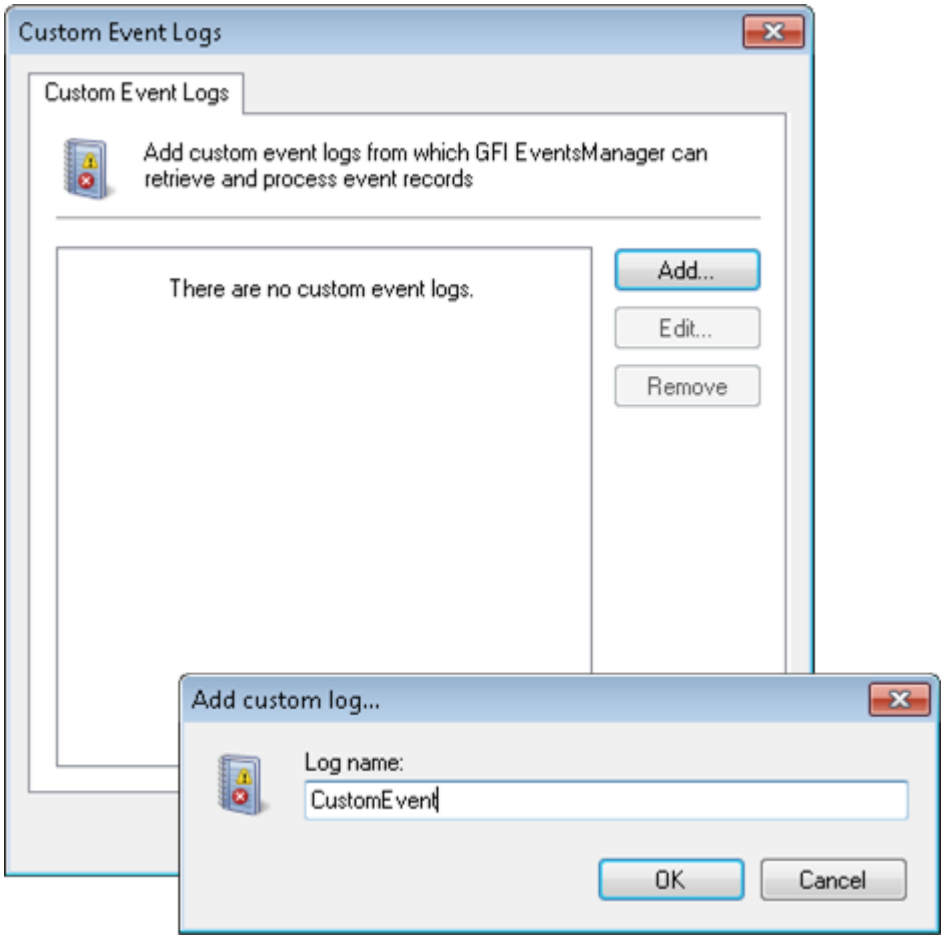
1. Click **Configuration** tab and select **Options**.

2. From the left pane, right-click on the **Custom Events Logs** node and select **Edit custom logs…**



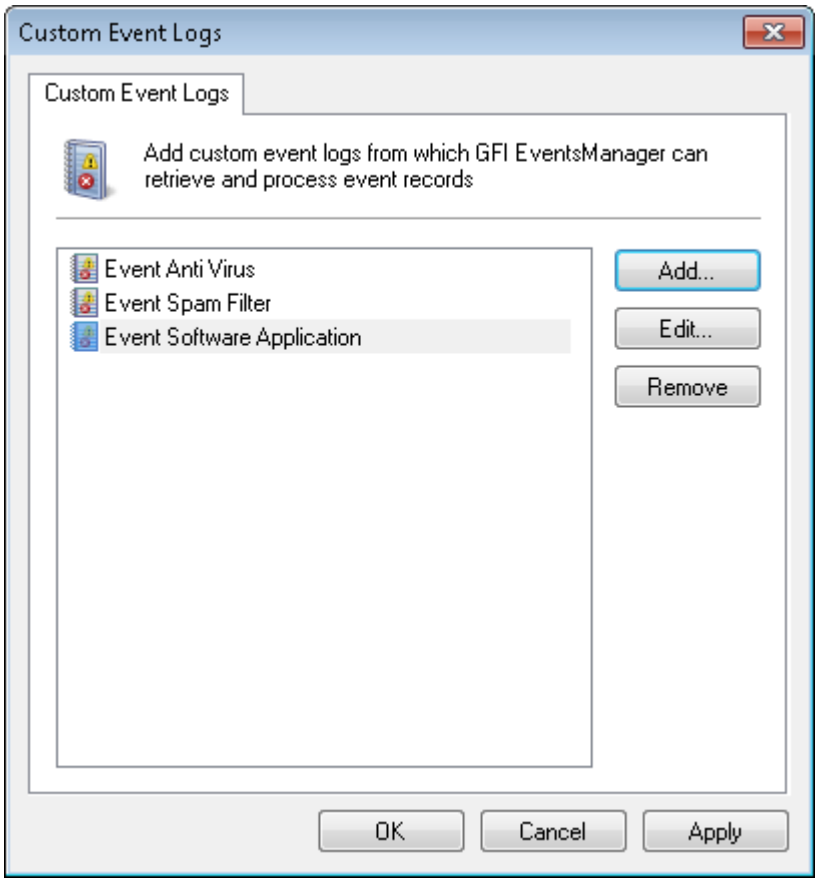
Screenshot 96 - Custom event logs setup

3. Click **Add...** button and specify the name of your custom event log.



Screenshot 97 - Custom event logs dialog

4. Click **OK** to finalize settings.

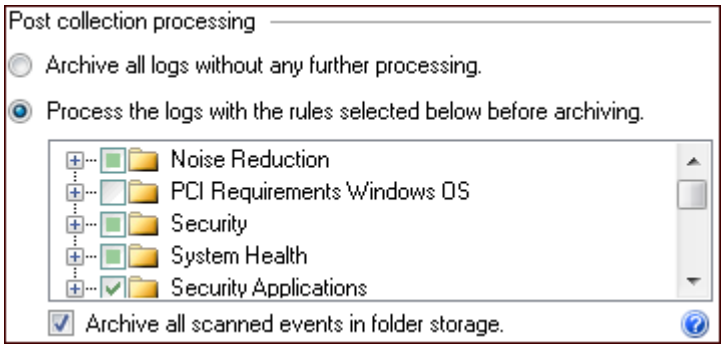


Screenshot 98 - List of custom events

5. (Optional) Click **Edit** to rename the selected custom event, or click **Remove** to delete the selected custom event.

7.4 Archiving events

By default, GFI EventsManager is configured to process all event logs collected from target computers.


Post collection processing
Archive all logs without any further processing.
Process the logs with the rules selected below before archiving.
Noise Reduction
PCI Requirements Windows OS
Security
System Health
Security Applications
Archive all scanned events in folder storage.

Screenshot 99 - Archiving events after processing

Processed events can be archived into the GFI EventsManager database backend and\or stored in a storage folder. By default, GFI EventsManager can be configured to automatically archive events:

- Based on their classification. For example, you can configure default settings which archive only critical events. For information on how to configure event archiving based on event classification refer to Configuring default classification actions section in this manual.
- Based on the conditions configured in the event processing rules. Rules provide an alternative and more flexible way to archive processed events. Through these rules, you can selectively archive only those events that satisfy specific rule condition(s) - regardless their classification. For example, you can configure a rule which archives only critical events with ID 537.

After collecting the events, GFI EventsManager can be configured to store the collected events into a storage folder, this can be done by selecting **Archive all scanned events in folder storage.** The storage folder path can be configured from the **Configuration** tab, for more information refer to Configure storage folder. This feature allows the administrator to store all the events in a storage folder and store only important events (that trigger rules) in the database.

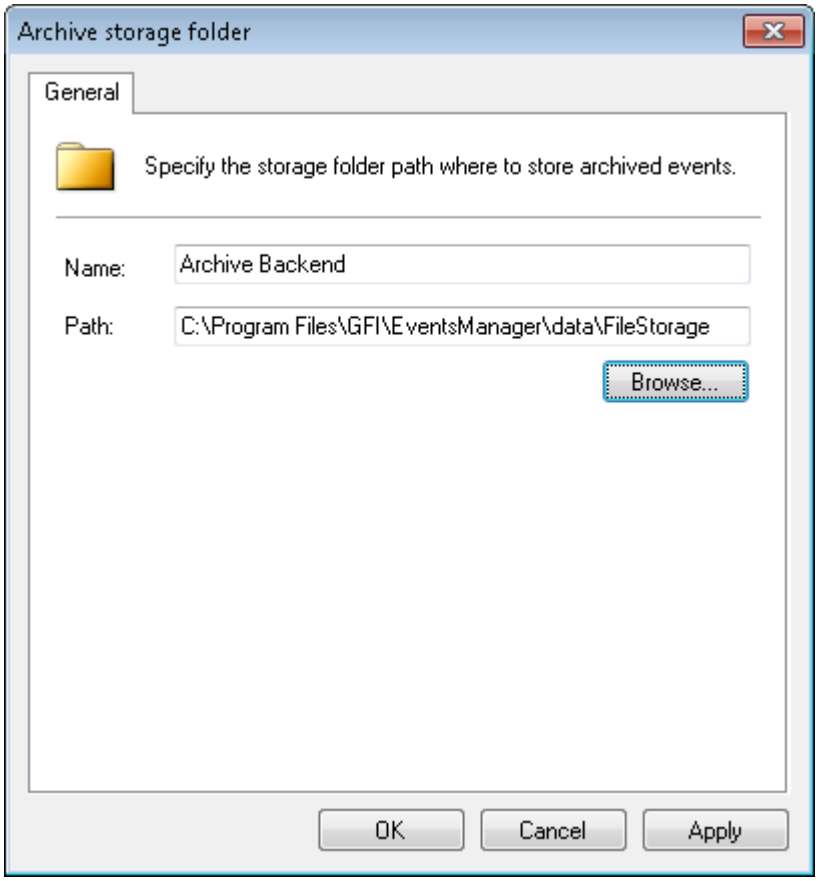
When configuring SNMP Trap Server port settings, make sure that the configured TCP or UDP port is not already in use by other installed applications. This may affect the delivery of SNMP Trap messages to GFI EventsManager.

For more information on how to retrieve archived events from the storage folder, refer to Import from file section in this manual.

7.4.1 Configure storage folder

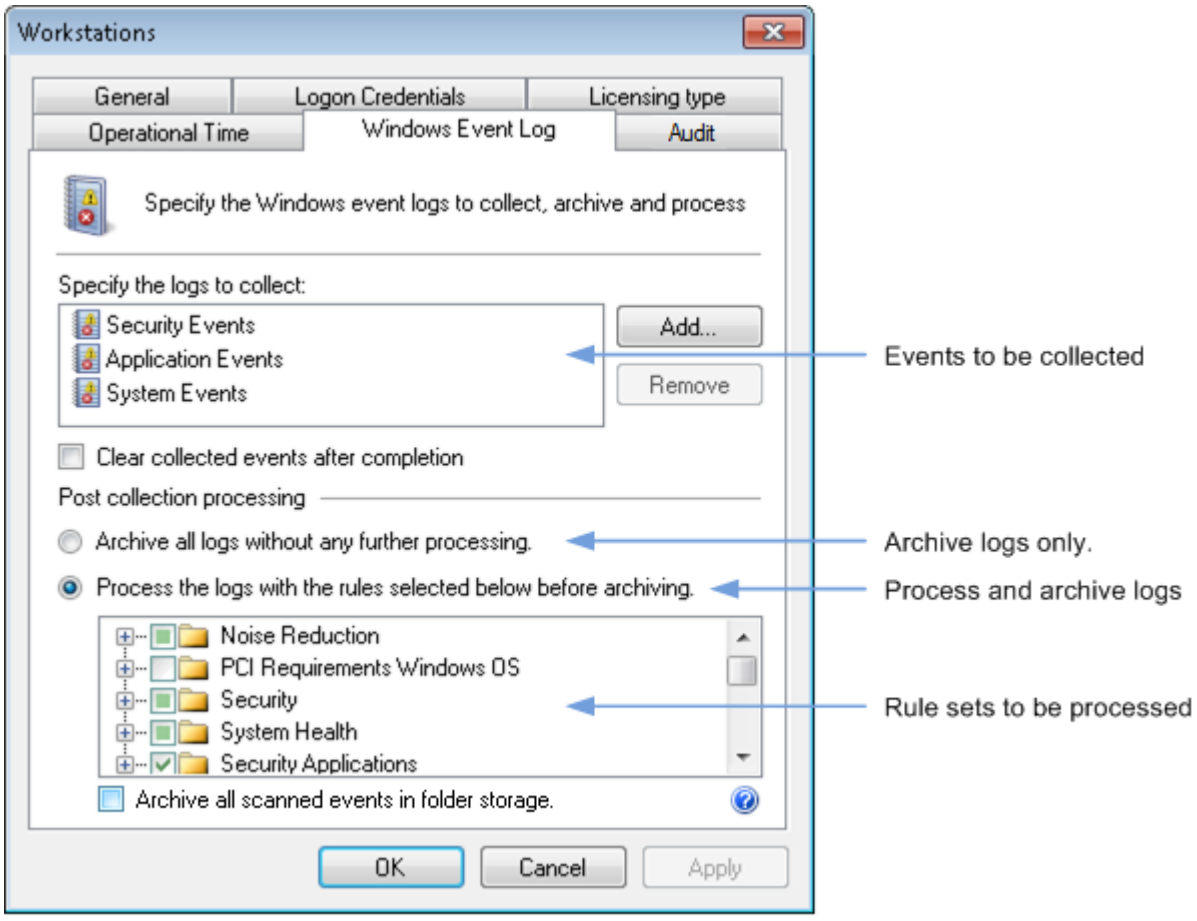
GFI EventsManager can be configured to archive events in a storage folder after applying processing rules. This feature allows the system to store all the events retrieved from event sources, on the local host (where GFI EventsManager is installed). To configure the storage folder:

1. Click **Configuration** tab ► **Options**.
2. From **Configurations** click **Database and Files Backend** node.
3. From the right panel click **Change database backend**.
4. Key in a name for the archive file.
5. Click **Browse** to locate the path where the archive file will be saved.
6. Click **OK** to apply settings.



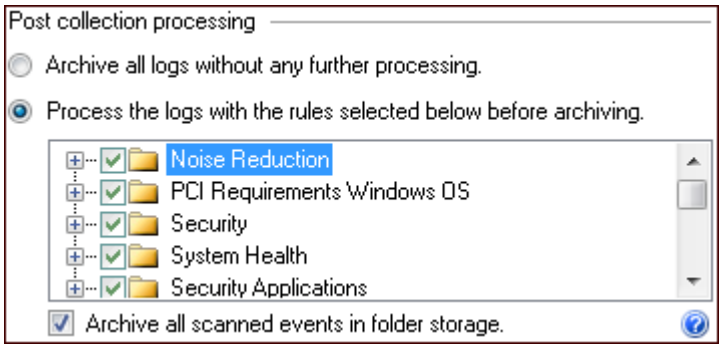
Screenshot 100 - Configure file folder

7.5 Select event processing rules



Screenshot 101 - Computer group properties: Configuring Windows Event Logs parameters

To process and classify events, specify which rules are applied against the collected logs. This is achieved by selecting the rule-sets folder or rule-set(s) that contain the required event processing rules.


Post collection processing
Archive all logs without any further processing.
Process the logs with the rules selected below before archiving.
Noise Reduction
PCI Requirements Windows OS
Security
System Health
Security Applications
Archive all scanned events in folder storage.

Screenshot 102 - Selecting event processing rules/rule-sets

However, you must pay attention and choose the right "rule" for the job. The rule-sets that ship with GFI EventsManager are pre-configured to specific logs; therefore it is imperative that you choose rule-sets that can effectively process the events recorded in the collected logs.

Certain rule-sets contain specialized rules that are event specific. Therefore these rules will only be effective when used to process such specific events; failing to do so will result into erroneous event processing, data loss and non-significant results. For example, the 'Monitoring and Attack detection' rule-set contains rules specifically built to process Windows Security events. Therefore it will not be very effective if used to process Windows application events.

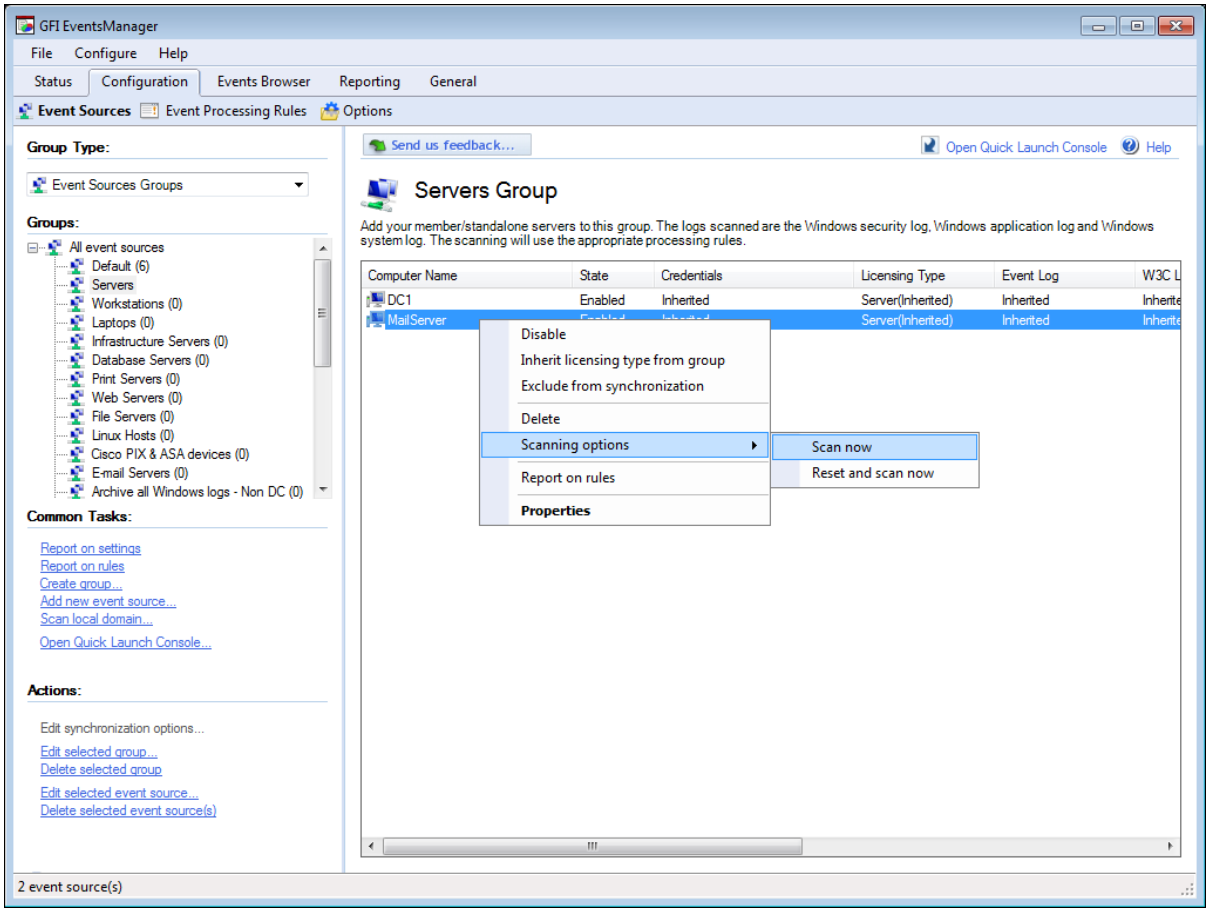
	By default, GFI EventsManager ships with pre-selected rules-sets/folders that can effectively process Windows Event Logs. If you are new to the product or you are not yet acquainted with the functionality of rule-sets, we recommend that you leave these settings as default.
	If no rules-sets are shown in the selection window, this means that no event processing rules exist for the type of log being configured. For more information on how to configure event processing rules and rule-sets, refer to Using event processing rules chapter.

7.6 Triggering event source scanning manually

In GFI EventsManager, you can manually trigger an event collection iteration on target computers. To achieve this:

1. Right-click on the computer group which contains the required event sources.

2. Select **Scanning options ► Scan now**.



Screenshot 103 - Triggering log collection manually

8 Manage rule-sets

8.1 Introduction

Event processing rules are the conditions which:

- Classify processed events
- Filter out noise (repeated events) or unwanted events
- Trigger email, SMS and network alerts on key events
- Attempt remedial actions by executing specific scripts and executable files on key events.
- GFI EventsManager ships with pre-configured rules that can be used to process events with minor configuration effort. You can also customize these default rules or create tailored ones for all supported log types (i.e. Windows Event Logs, W3C, Syslog, SNMP Traps and SQL Server audit logs).

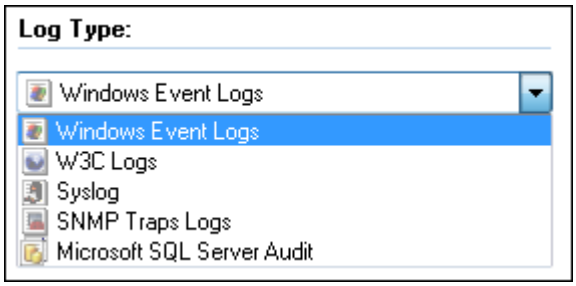
In GFI EventsManager, event processing rules are organized into rule-sets, which in turn are stored in rule-set folders. Table 27 below lists some of the most common rule-set folders in GFI EventsManager.

Table 27 - Rule-set folders available in GFI EventsManager

RULE-SET FOLDER	DESCRIPTION
Noise reduction rules	Contains rules tailored for the removal of repeated events and other noise from logs.
PCI requirements Windows OS	Contains rules tailored for PCI DSS compliance
Security	Contains rules tailored for the processing of Security logs and System logs.
System Health	Contains rules tailored for the processing of Application logs and System logs.
Security Applications	Contains rules tailored for the processing of Application logs, Security logs and System logs.
Infrastructure Server	Contains rules tailored for the processing of Application logs, DNS logs and System logs.
Database Server	Contains rules tailored for the processing of Application logs.
Web Server	Contains rules tailored for the processing of Application logs and System logs.
Print Server	Contains rules tailored for the processing of Application logs and System logs.
GFI Rules	Contains rules for processing GFI LANguard vulnerability scans and GFI EventsManager auditing results.
Terminal Services	Contains rules tailored for the processing of events generated terminal device driver services.
Email Server	Contains rules tailored for the processing of events generated by Microsoft Exchange server.
File Replication	Contains rules tailored for the processing of events generated by file replication services.
Directory Server	Contains rules tailored for the processing of events found in the Directory Services log.
HTTP protocol logs	Contains rules tailored for the processing of HTTP events logged by IIS Web Server(s)
FTP protocol logs	Contains rules tailored for the processing of FTP events logged by IIS Web server(s)

RULE-SET FOLDER	DESCRIPTION
SMTP protocol logs	Contains rules tailored for to monitor events logged by ISS SMTP server(s).
Linux/Unix	Contains rules tailored for the processing of Syslogs.
Cisco PIX & ASA	Contains rules tailored for the processing of events generated by Cisco PIX firewalls and Cisco Adaptive Security Appliances
Database changes	Contains rules tailored for the processing of events generated when a database schema is changed.
SQL Server errors	Contains rules tailored for processing of events generated when an SQL error occurs.
SharePoint Audit	Contains rules tailored for processing events generated by SharePoint activity.

8.2 Managing rule set folders



Screenshot 104 - The log type drop-down list

8.2.1 Add a rule-set folder

To create a new rule-set folder:

1. Click **Configuration** tab and select **Event Processing Rules**.
2. From **Log Type**, select the log-type for which you will be creating the rule-set folder.
3. From **Common Tasks**, select **Create folder**.
4. Specify a unique name for the new rule-set folder.

8.2.2 Renaming and deleting folders

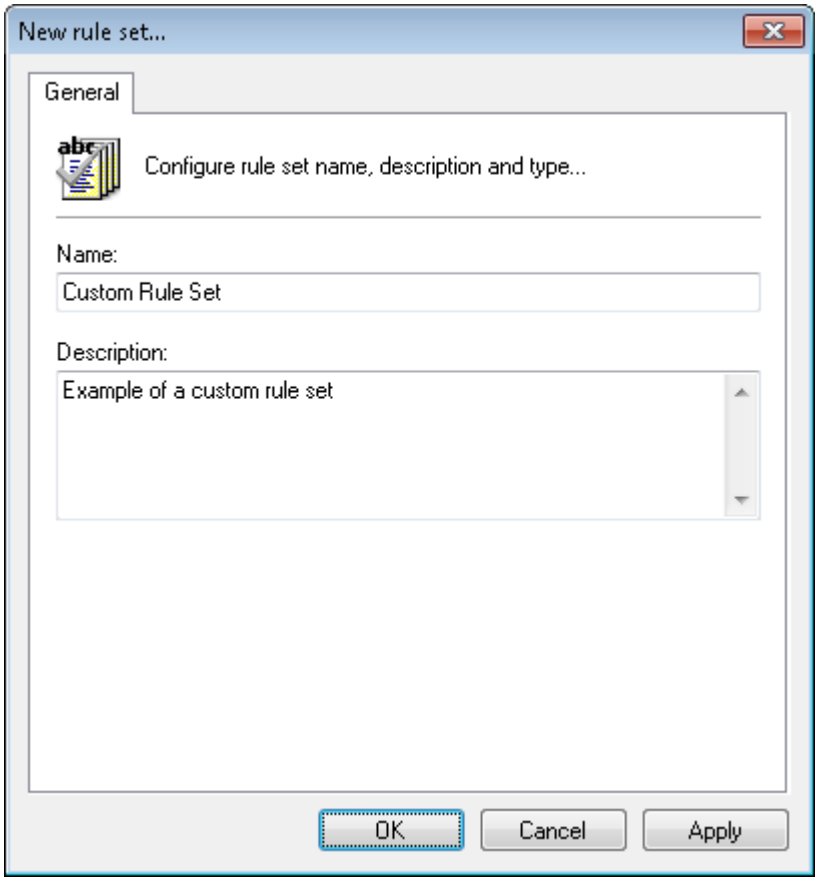
To rename or delete existing rule-set folders, right-click on the target rule-set folder and select **Rename** or **Delete** accordingly.

Deleting a rule-set folder will lead to the deletion of all the rules and rule-sets contained within the deleted folder.

8.2.3 Creating a new rule-set

To create a new rule-set:

1. Click **Configuration** tab and select **Event Processing Rules**.
2. From **Log Type**, select the log-type for which you will be creating the new rule-set.
3. Right-click on the folder where to create the new rule-set and select **Create new rule set...**.



Screenshot 105 - New rule-set dialog box

4. Specify a name and a description for this new rule-set.

5. Click **OK** to finalize your settings.

8.2.4 Editing a rule-set

To edit rule-set parameters:

1. Right-click on the rule-set to edit and select **Properties**.

2. Make the required changes and click **OK** to finalize your settings.

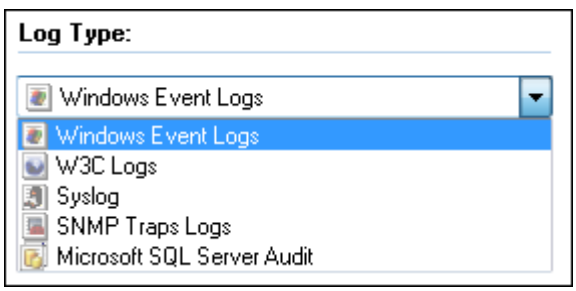
To delete a rule-set, right-click on the rule-set and select **Delete.**

8.3 Create log rules

8.3.1 Creating a new Windows Event Log rule

To create a new rule which is only applicable to Windows Event Logs:

1. Click **Configuration** tab and select **Event Processing Rules**.

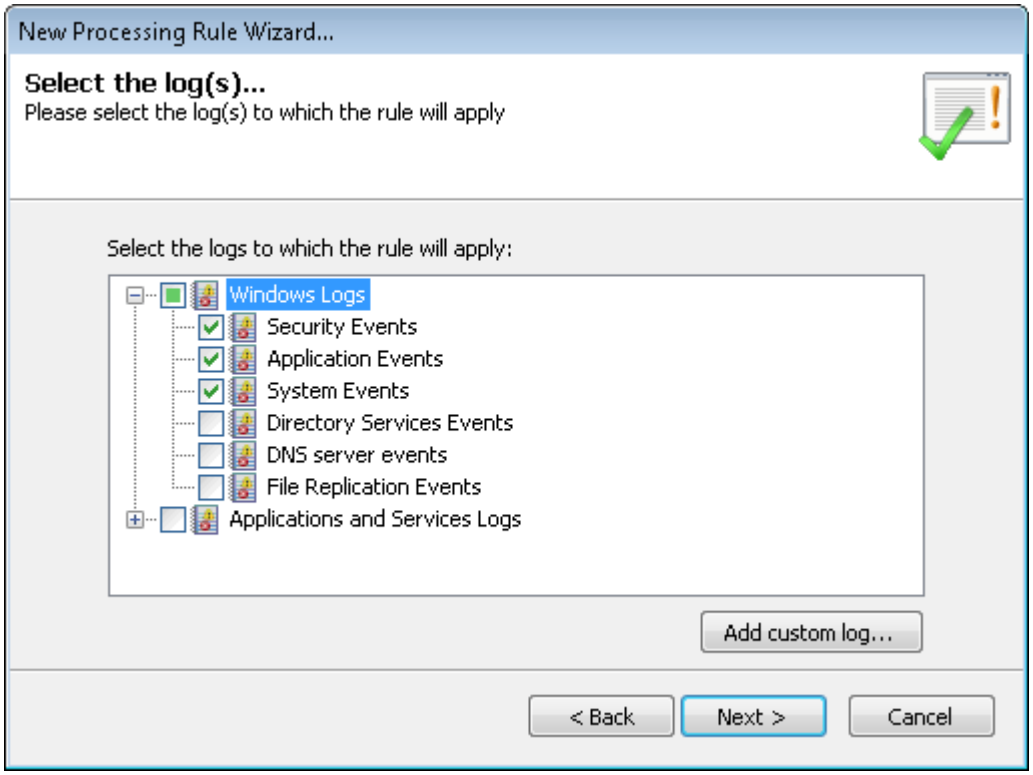


Screenshot 106 - Selecting log-type from the provided drop-down

2. Select **Windows Event Logs** from the drop down list.

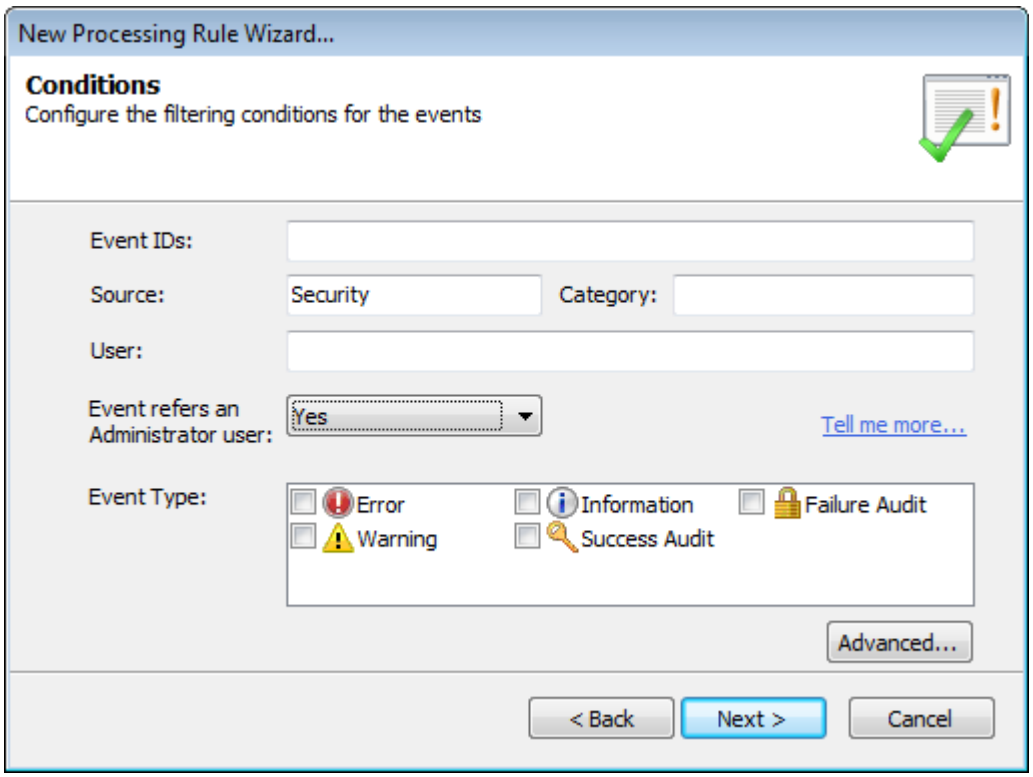
3. Right-click the rule-set where the log rule will be created and click **Create new rule...**

4. Specify the name and a description for the new rule. Click **Next** to proceed with the configuration.



Screenshot 107 - GFI EventsManager: Select the Log(s)

5. Select the event logs to which the rule applies and click **Next**.

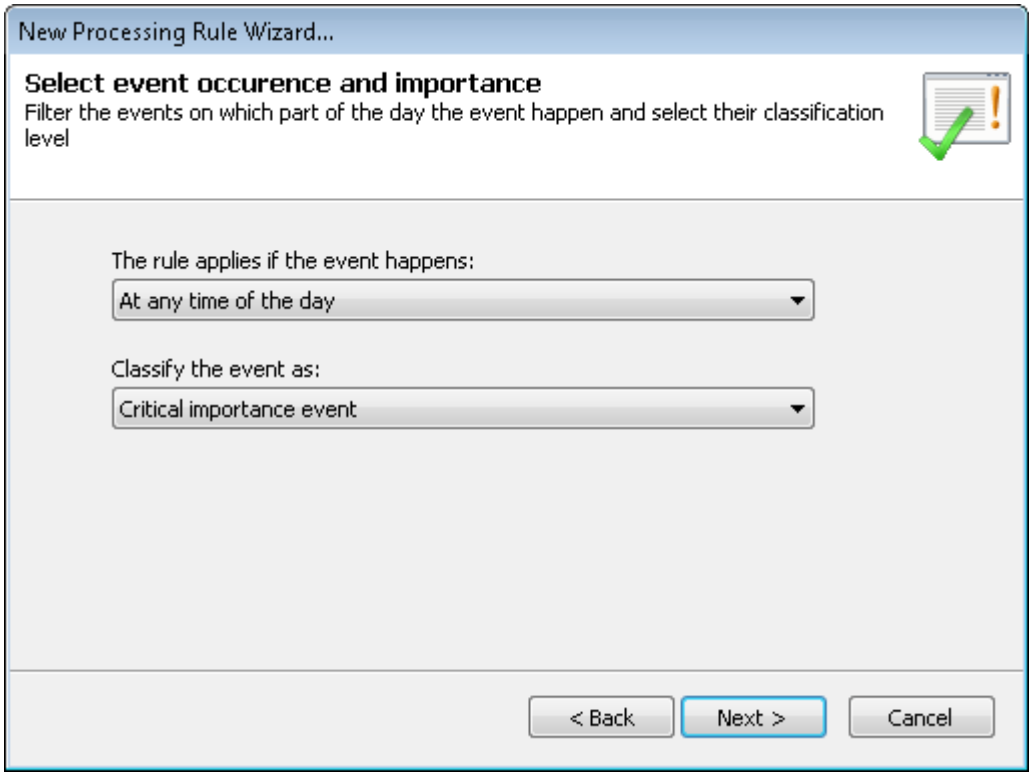


Screenshot 108 - GFI EventsManager: Select the filtering conditions

6. Configure the event filtering conditions of this rule. To create a rule which will be applied to all events, leave the event ID empty. Click **Next** to continue.

To filter events that refer to an administrator user (events having the security identifier SID that identifies a logon administrator session), ensure that if the target is a domain member, the domain controller must be added as a target machine and scanned. For more information on how to add target machine, refer to Managing event sources groups section in this manual.

7. (Optional) Click **Advanced** to configure advanced filtering conditions. For more information refer to Advanced event filtering parameters section in this manual.

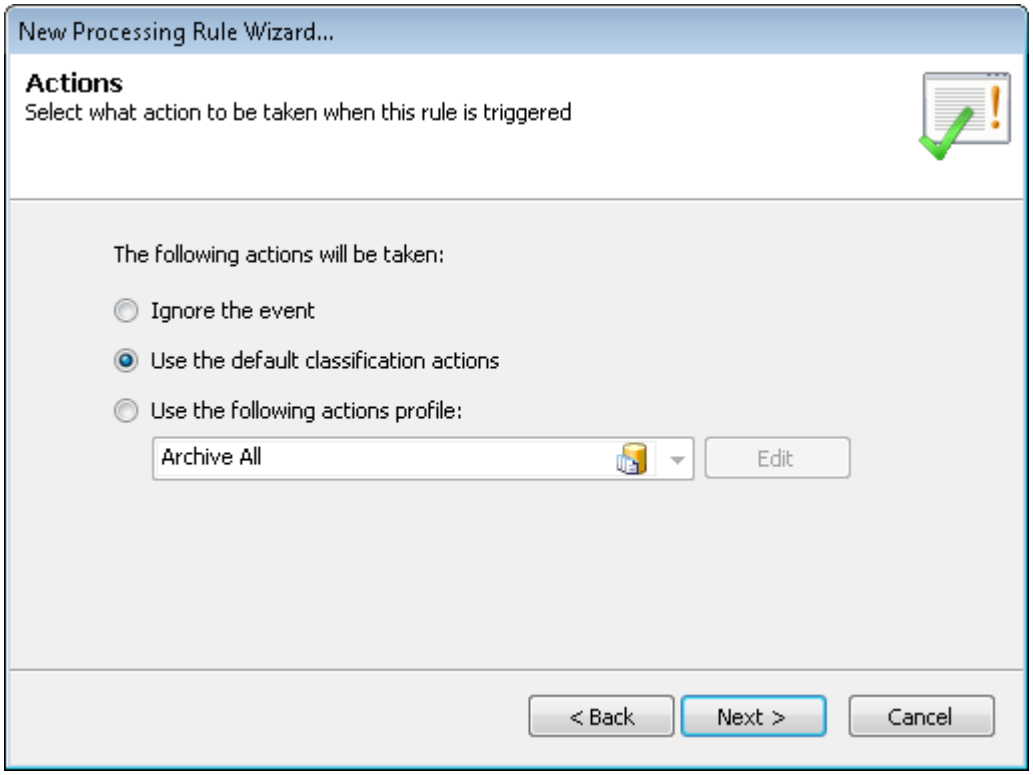

New Processing Rule Wizard...
Select event occurence and importance
Filter the events on which part of the day the event happen and select their classification level
The rule applies if the event happens:
At any time of the day
Classify the event as:
Critical importance event
< Back
Next >
Cancel

Screenshot 109 - New processing rule wizard: Select event occurrence and importance

8. Specify the time when this rule will be executed. (Example: anytime, during working hours or outside working hours).

Working and non-working hours are based on the operational time parameters configured for your event sources. For more information on how to configure operational times, refer to Configure operational time chapter.

9. Select the classification (critical, high, medium, low or noise) that will be assigned to events that satisfy the conditions in this rule. Click **Next** to continue.



Screenshot 110 - New processing rule wizard: Select action

10. Specify which actions will be triggered by this rule. Actions available are:

Ignore the event

Use the default classification actions

Use an action profile.

If **Use the following actions profile** is selected, click **Edit** to configure and select actions to perform.

11. Click **Next** to proceed to the final dialog. Click **Finish** to finalize your settings.

Newly created rules are disabled by default and will **NOT** become operational unless enabled. For information on how to enable event processing rules refer to section in this Manual.

8.3.2 Creating a new W3C rule

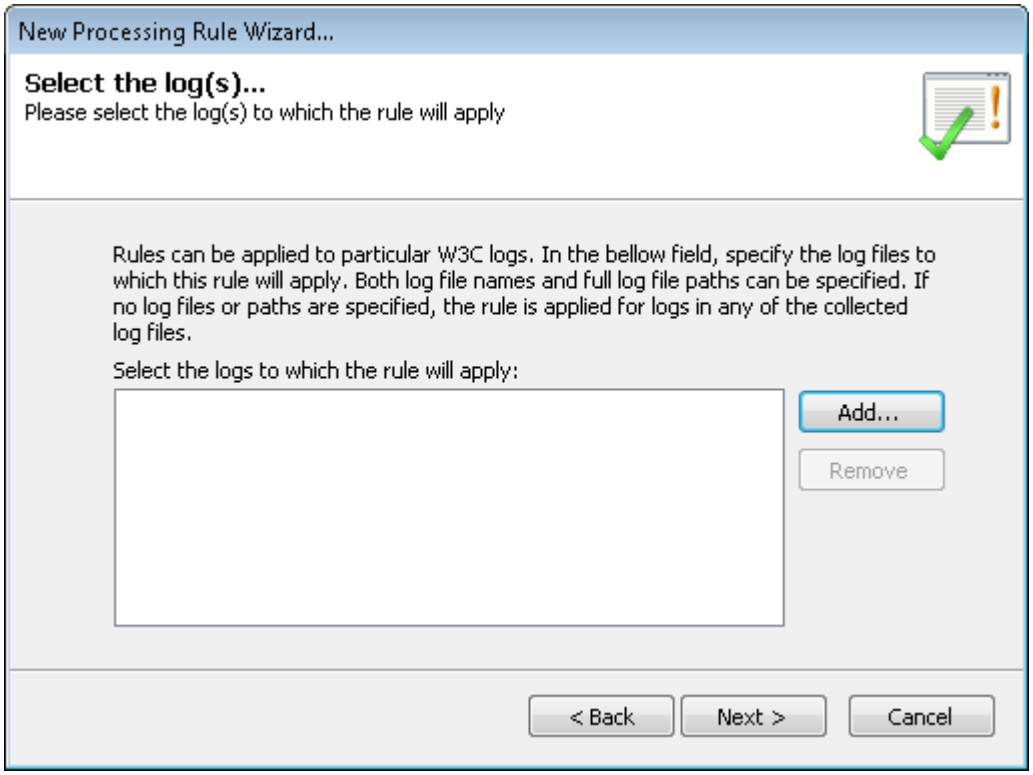
To create a new rule which is only applicable for W3C logs:

1. Click **Configuration** tab and select **Event Processing Rules**.

2. From **Log Type**, select **W3C Logs**.

3. Right-click on the rule-set in which you will be creating the new rule and select **Create new rule…**

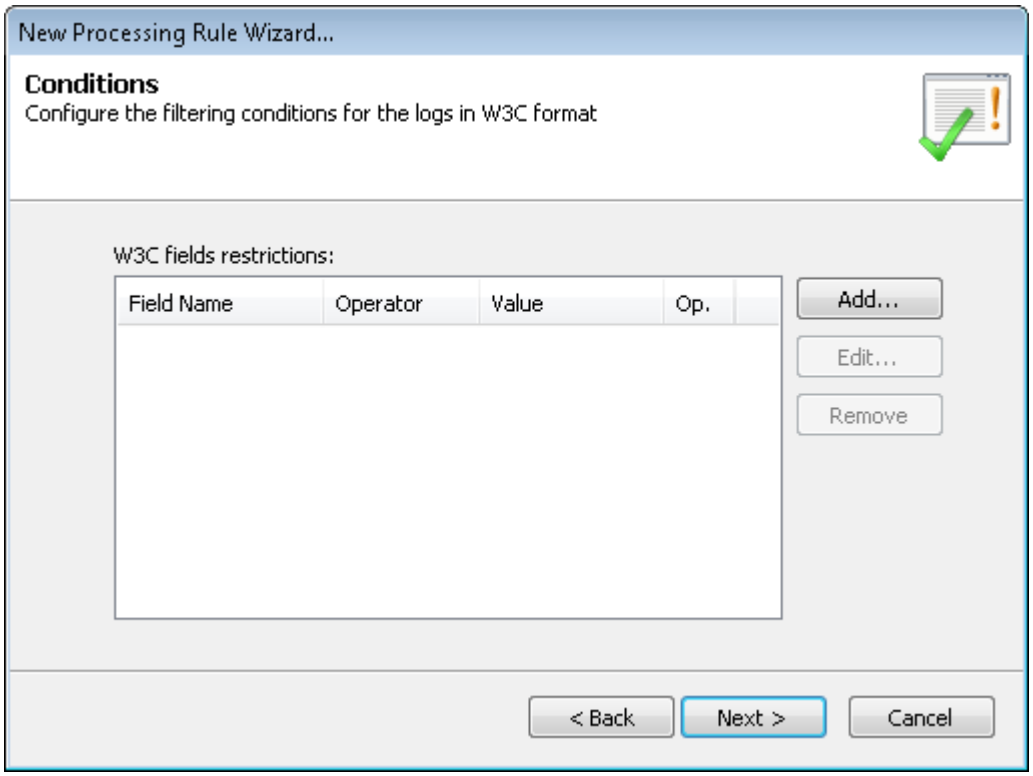
4. Specify a name and description for the new rule. Click **Next** to proceed with the configuration.


New Processing Rule Wizard...
Select the log(s)...
Please select the log(s) to which the rule will apply
Rules can be applied to particular W3C logs. In the bellow field, specify the log files to which this rule will apply. Both log file names and full log file paths can be specified. If no log files or paths are specified, the rule is applied for logs in any of the collected log files.
Select the logs to which the rule will apply:
Add...
Remove
< Back
Next >
Cancel

Screenshot 111 - New processing rule wizard: Select W3C Log

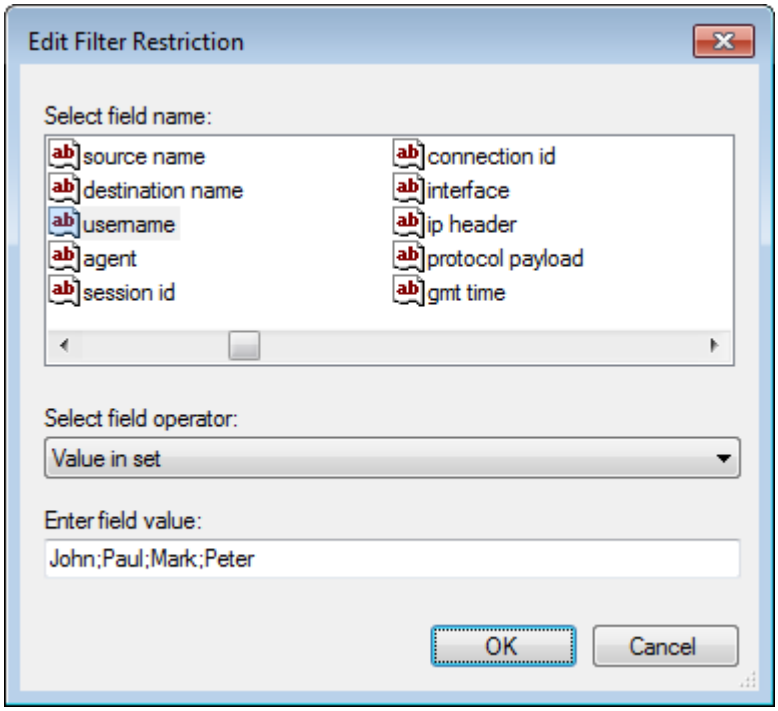
5. Click **Add** button. Specify the path to the W3C logs for which this rule applies or leave blank to apply this rule to all W3C logs. Click **Next** to continue.

Multiple paths can be specified during configuration.

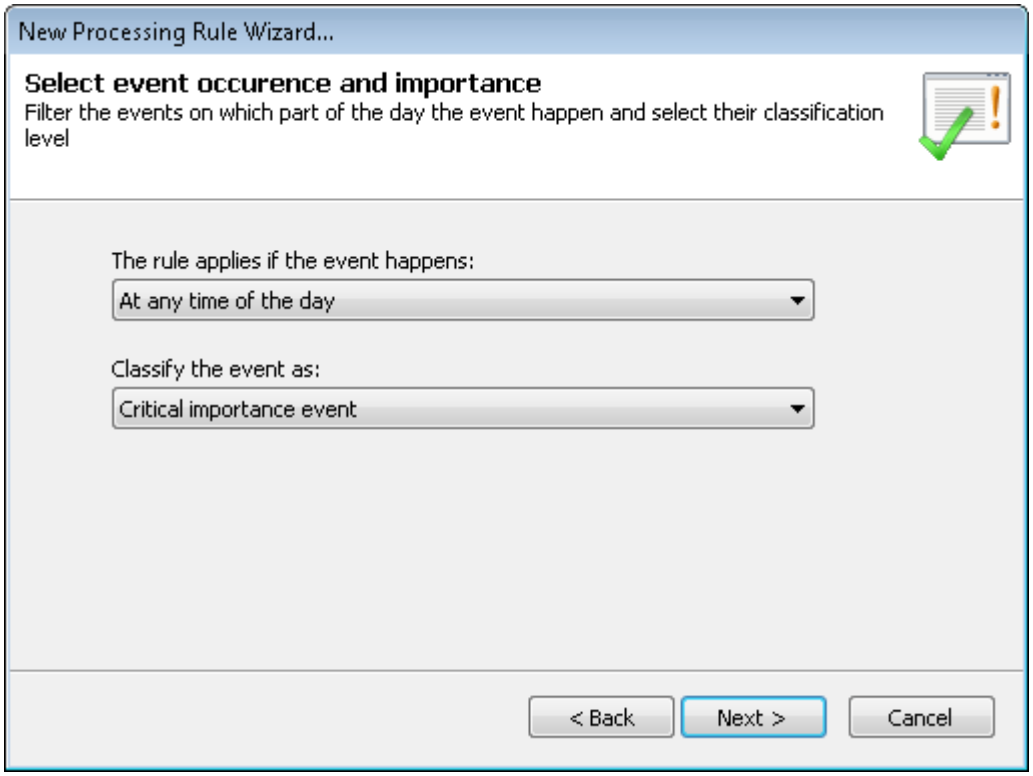


Screenshot 112 - New processing rule wizard: Configure filtering conditions.

6. Click **Add** button and configure event filtering conditions. Repeat until all conditions have been specified. Click **Next** to continue.



Screenshot 113 - Edit filter rules

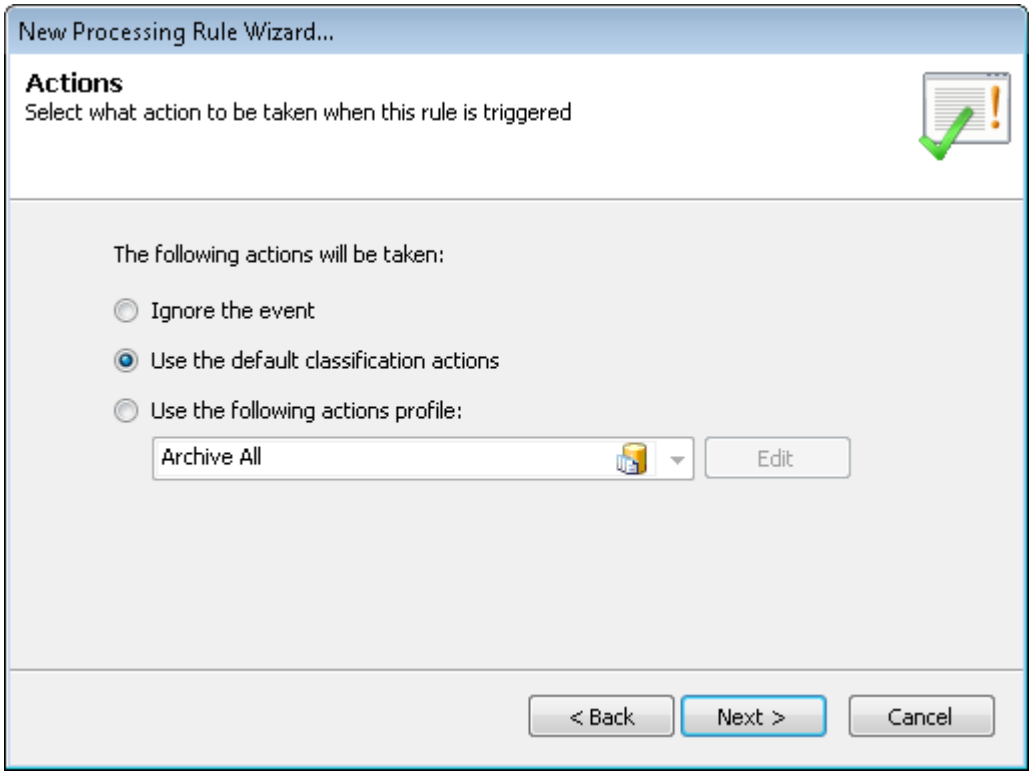

New Processing Rule Wizard...
Select event occurence and importance
Filter the events on which part of the day the event happen and select their classification level
The rule applies if the event happens:
At any time of the day
Classify the event as:
Critical importance event
< Back
Next >
Cancel

Screenshot 114 - New processing rule wizard: Select event occurrence and importance

7. Specify the time when this rule will be executed. (i.e. anytime, during working hours or outside working hours).

Working and non-working hours are based on the operational time parameters configured for your event sources. For more information on operational times, refer to Using event processing rules section in this manual.

8. Select the classification (critical, high, medium, low or noise) that will be assigned to events that satisfy the conditions in this rule. Click **Next** to continue.



Screenshot 115 - New processing rule wizard: Select action

9. Specify which actions will be triggered by this rule. You can choose to ignore the event, trigger the default action, or customize alerts.

10. Click **Next** to proceed to the final dialog. Click **Finish** to finalize your settings.

Newly created rules are disabled by default and will NOT become operational unless enabled. For information on how to enable event processing rules refer to Collecting events section in this Manual.

8.3.3 Creating a new Syslog rule

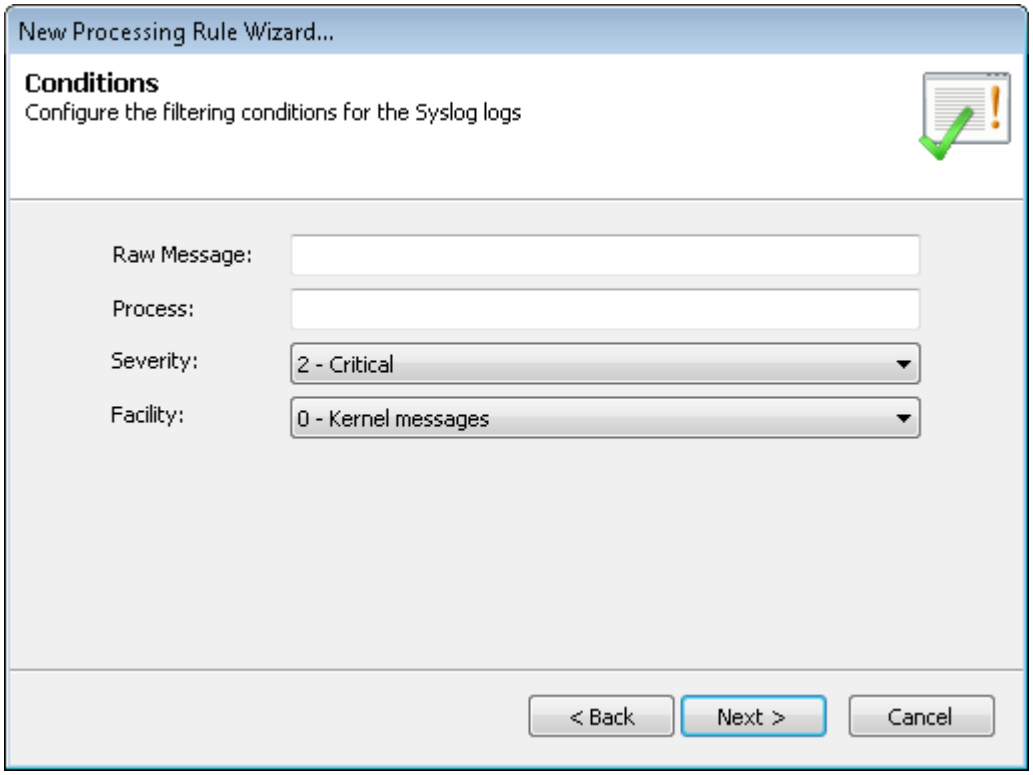
To create a new rule that is only applicable for the processing of Syslog messages:

1. Click **Configuration** tab and select **Event Processing Rules**.

2. From the **Log Type**, select **Syslog**.

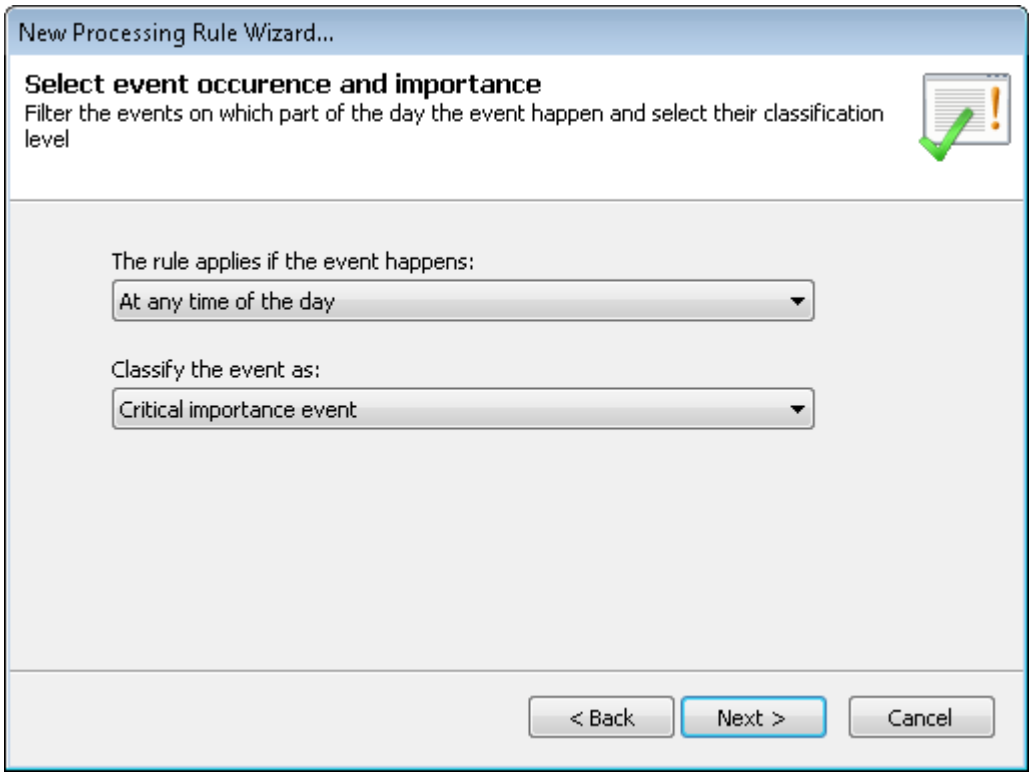
3. Right-click on the rule-set in which you will be creating the new rule and select **Create new rule…**

4. Specify the name and a description for the new rule. Click **Next** to proceed with the configuration.



Screenshot 116 - New processing rule wizard: Configure Conditions

5. Specify the log filtering conditions to be processed by this rule. When all conditions have been specified, click **Next**.

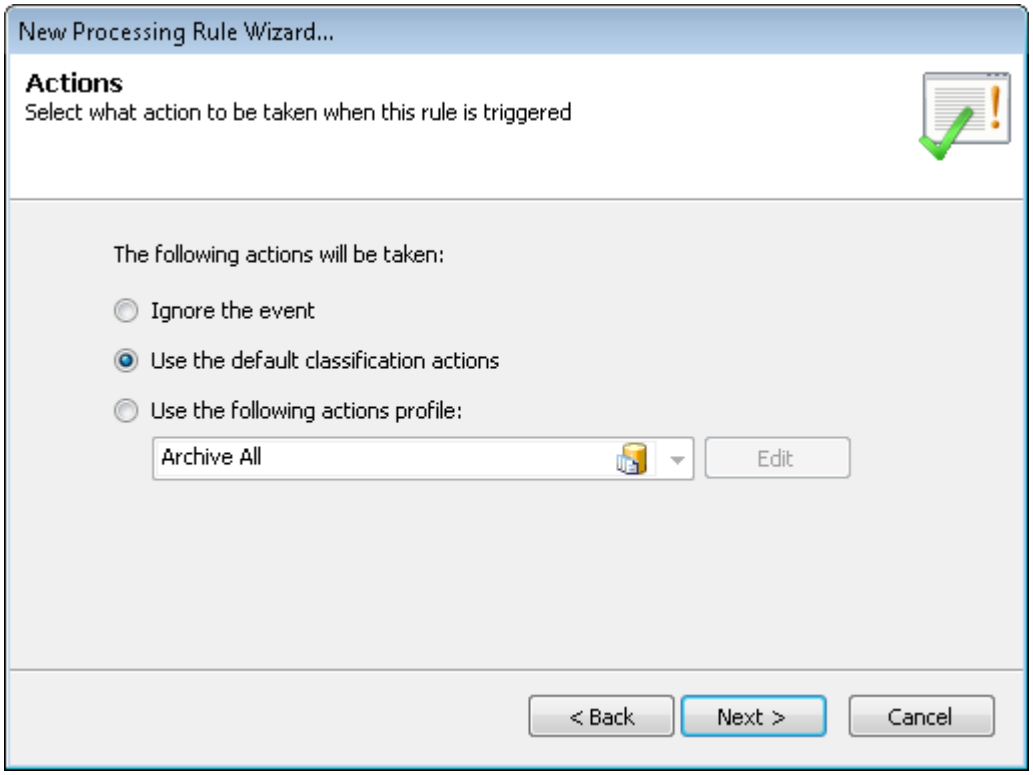

New Processing Rule Wizard...
Select event occurence and importance
Filter the events on which part of the day the event happen and select their classification level
The rule applies if the event happens:
At any time of the day
Classify the event as:
Critical importance event
< Back
Next >
Cancel

Screenshot 117 - New processing rule wizard: Select event occurrence and importance

6. Specify the time when this rule will be executed. (Example: anytime, during working hours or outside working hours).

Working and non-working hours are based on the operational time parameters configured for your event sources. For more information on operational times, refer to Configure operational time section in this manual.

7. Select the classification (critical, high, medium, low) that will be assigned to events that satisfy this rule. Click **Next** to continue.



Screenshot 118 - New processing rule wizard: Select action

8. Specify which actions will be triggered by this rule. You can choose to ignore the event, trigger the default action, or customize alerts.

9. Click **Next** to proceed to the final dialog. Click **Finish** to finalize your settings.

Newly created rules are disabled by default, hence will NOT become operational unless enabled. For information on how to enable event processing rules refer to Collecting Syslogs section in this Manual.

8.3.4 Creating a new SNMP Trap rule

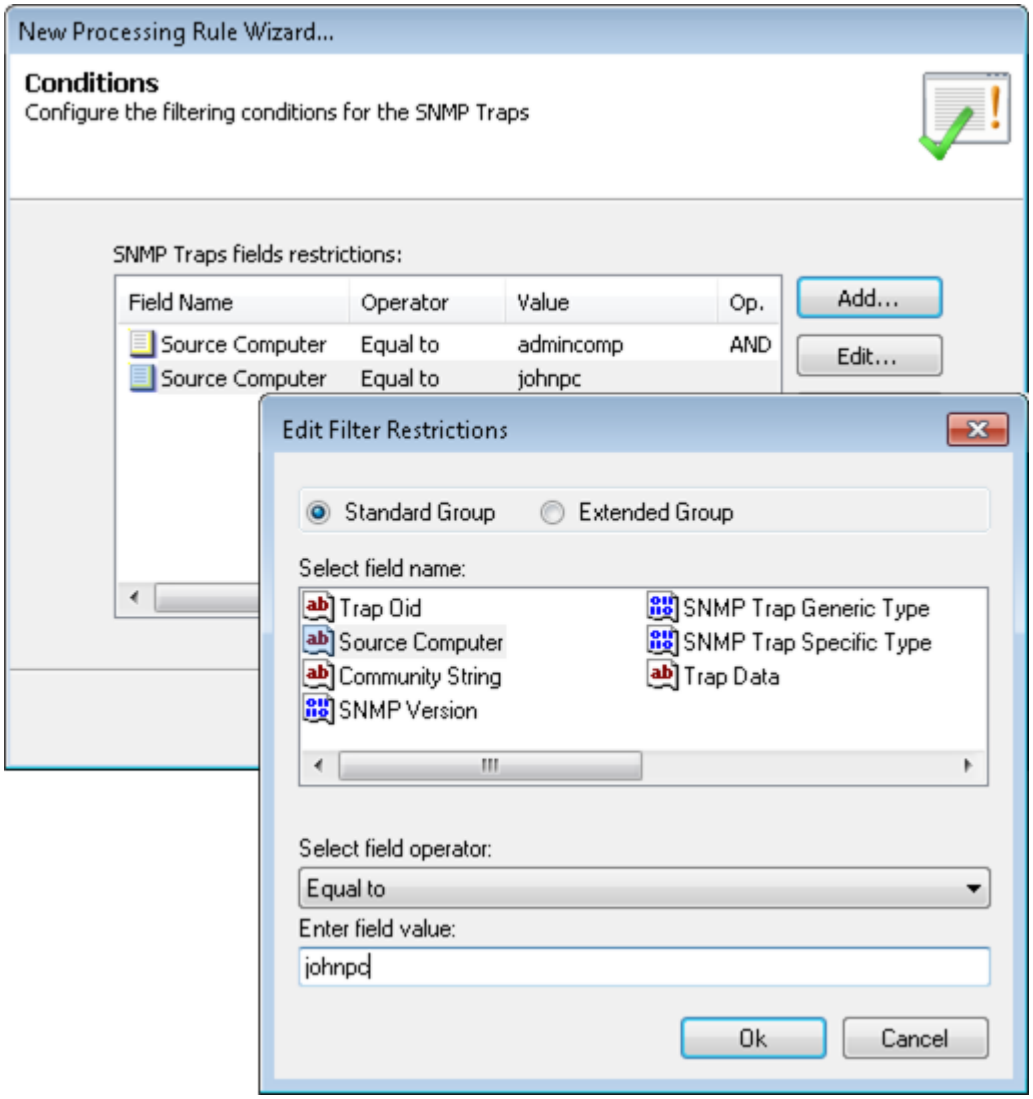
To create a new rule that is only applicable for the processing of SNMP Traps:

1. Click **Configuration** tab and select **Event Processing Rules**.

2. From **Log Type**, select **SNMP Traps logs**.

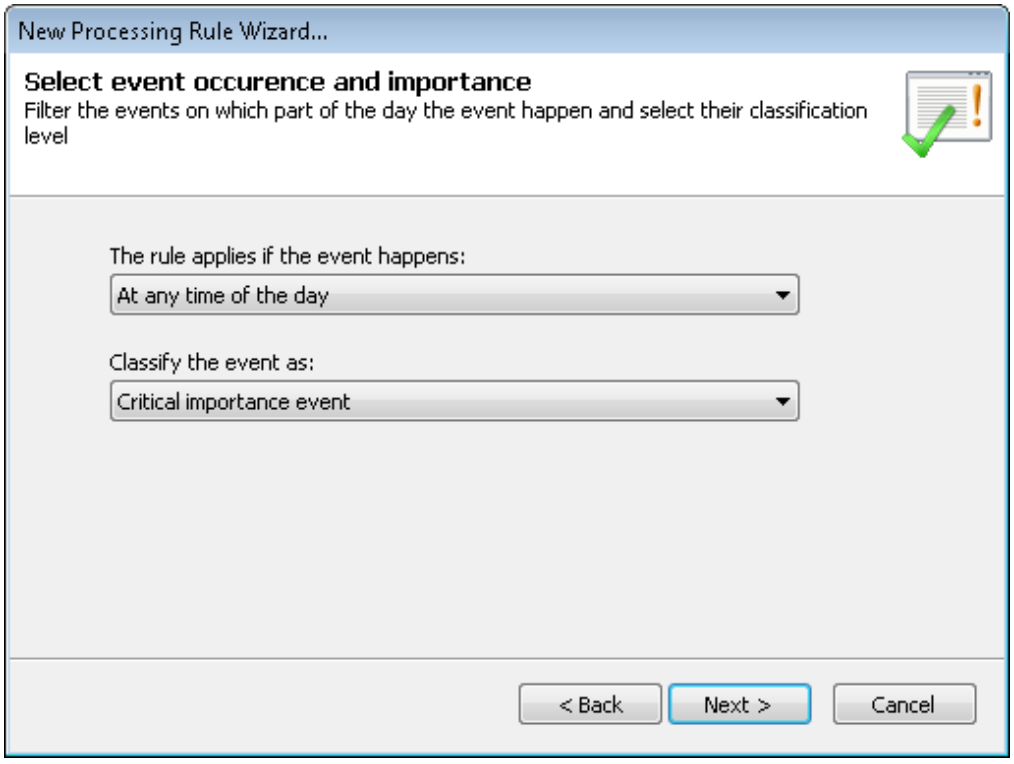
3. Right-click on the rule-set in which you will be creating the new rule and select **Create new rule…**

4. Specify the name and a description for the new rule. Click **Next** to proceed with the configuration.



Screenshot 119 - New processing rule wizard: Configure Conditions

5. Specify the log filtering conditions to be processed by this rule. When all conditions have been specified, click **Next**.

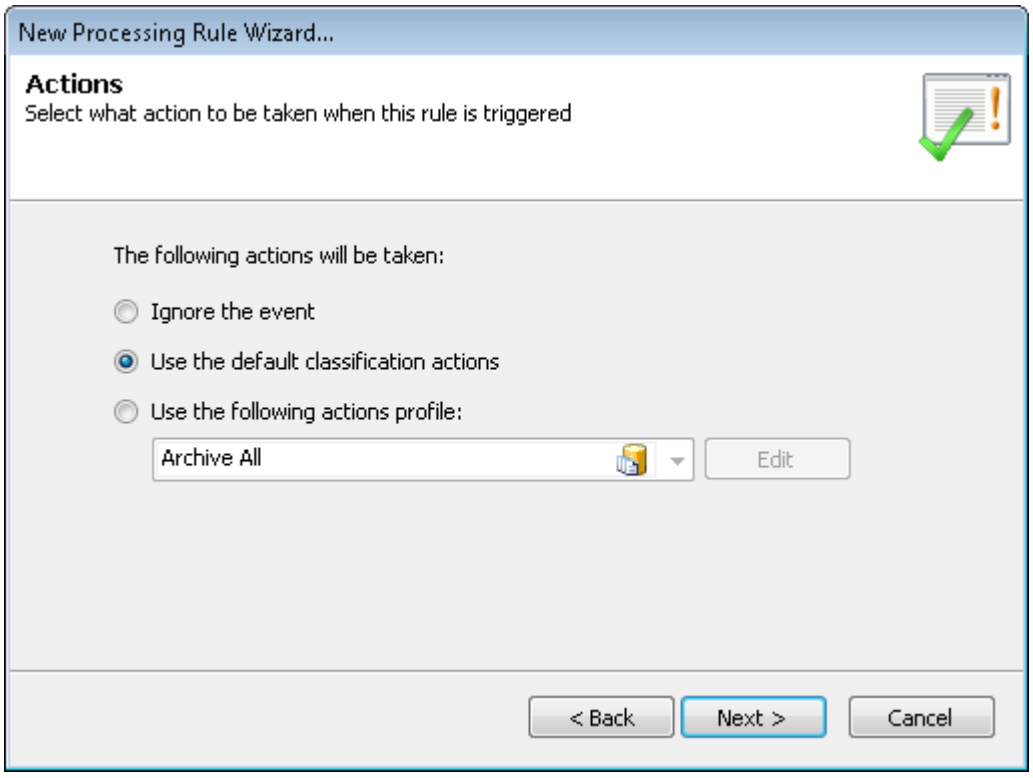

New Processing Rule Wizard...
Select event occurence and importance
Filter the events on which part of the day the event happen and select their classification level
The rule applies if the event happens:
At any time of the day
Classify the event as:
Critical importance event
< Back
Next >
Cancel

Screenshot 120 - New processing rule wizard: Select event occurrence and importance

6. Specify the time when this rule will be executed. (i.e. anytime, during working hours or outside working hours).

Working and non-working hours are based on the operational time parameters configured for your event sources. For more information on operational times, refer to Configure operational time section.

7. Select the classification (critical, high, medium, low) that will be assigned to events that satisfy this rule. Click **Next** to continue.



Screenshot 121 - New processing rule wizard: Select action

8. Specify which actions will be triggered by this rule. You can choose to ignore the event, trigger the default action, or customize alerts.

9. Click **Next** to proceed to the final dialog. Click **Finish** to finalize your settings.

Newly created rules are disabled by default, hence will NOT become operational unless enabled. For information on how to enable event processing rules refer to Collecting SNMP Traps section in this Manual.

8.3.5 Creating a new SQL Server audit log

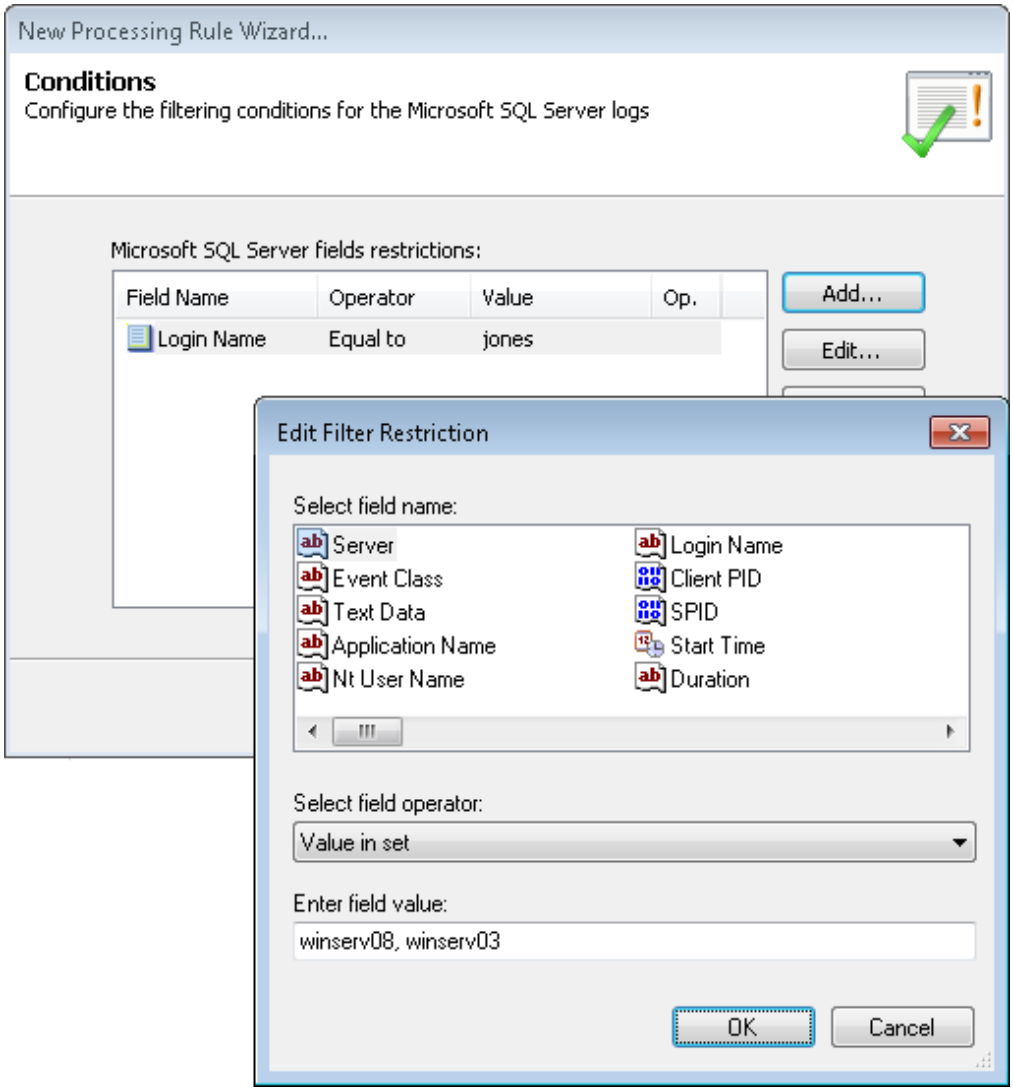
To create a new rule that is only applicable for the processing of SQL Server audit logs:

1. Click **Configuration** tab and select **Event Processing Rules**.

2. From **Log Type**, select **Microsoft SQL Server audit**.

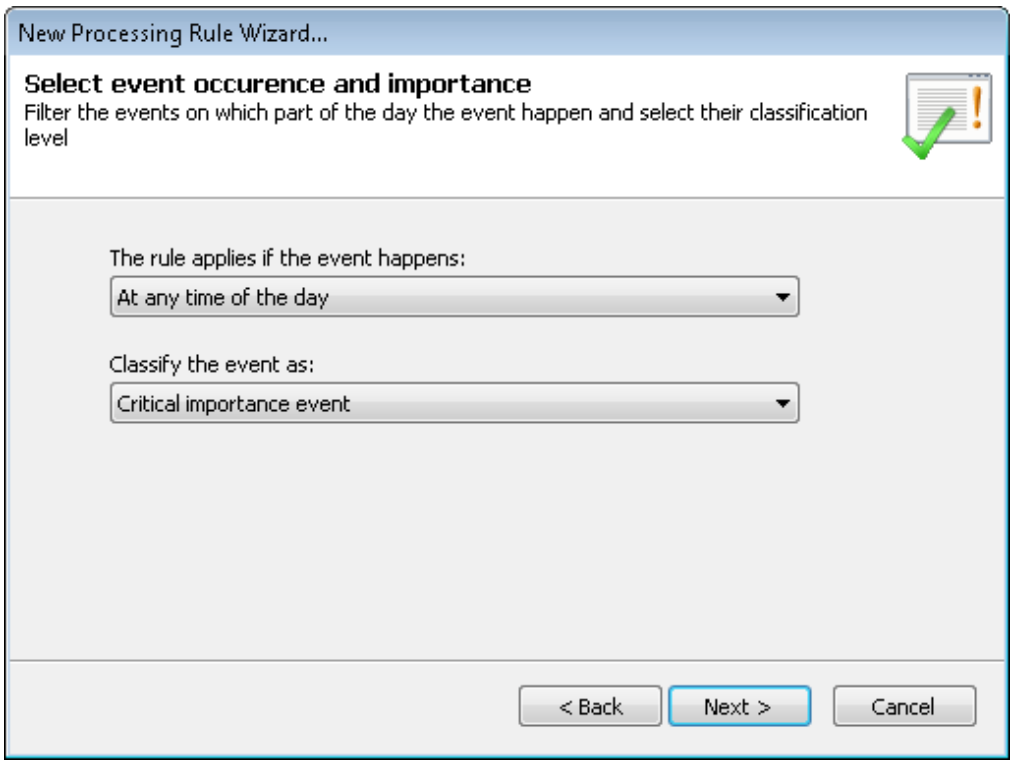
3. Right-click on the rule-set in which you will be creating the new rule and select **Create new rule…**

4. Specify the name and a description for the new rule. Click **Next** to proceed with the configuration.



Screenshot 122 - New processing rule wizard: Configure Conditions

5. Specify the log filtering conditions to be processed by this rule. When all conditions have been specified, click **Next**.

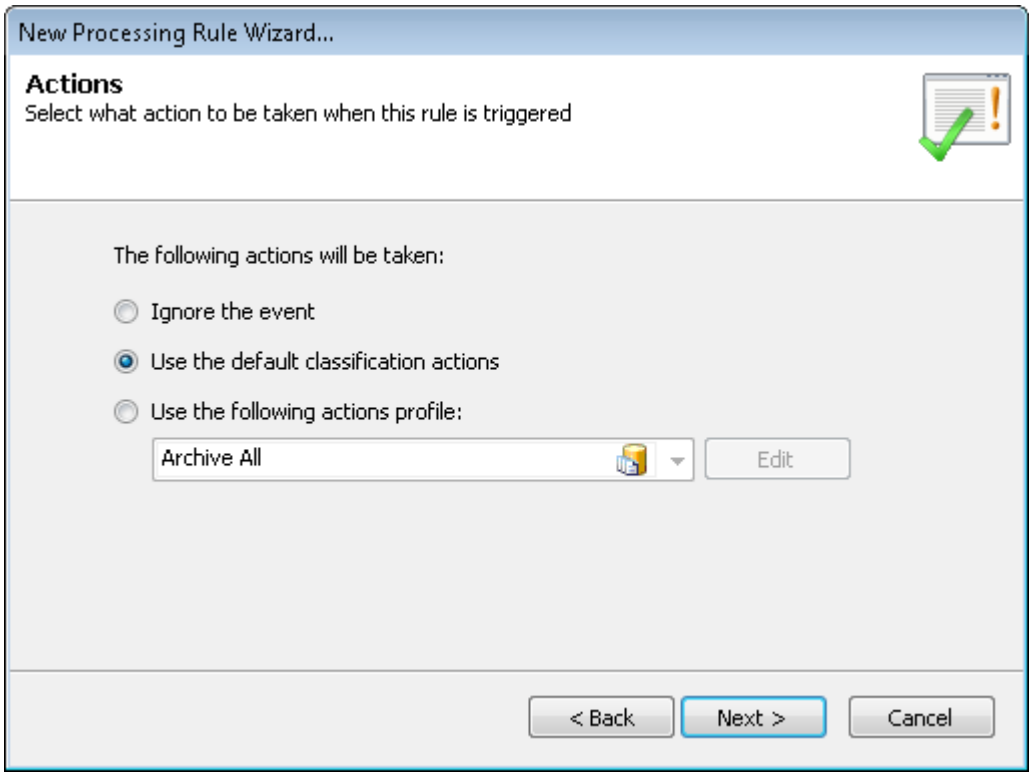

New Processing Rule Wizard...
Select event occurence and importance
Filter the events on which part of the day the event happen and select their classification level
The rule applies if the event happens:
At any time of the day
Classify the event as:
Critical importance event
< Back
Next >
Cancel

Screenshot 123 - New processing rule wizard: Select event occurrence and importance

6. Specify the time when this rule will be executed. (i.e. anytime, during working hours or outside working hours).

Working and non-working hours are based on the operational time parameters configured for your event sources. For more information on operational times, refer to Configure operational time section.

7. Select the classification (critical, high, medium, low) that will be assigned to events that satisfy this rule. Click **Next** to continue.



Screenshot 124 - New processing rule wizard: Select action

8. Specify which actions will be triggered by this rule. You can choose to ignore the event, trigger the default action, or customize alerts.

9. Click **Next** to proceed to the final dialog. Click **Finish** to finalize your settings.

8.3.6 Create new rule from an existing event

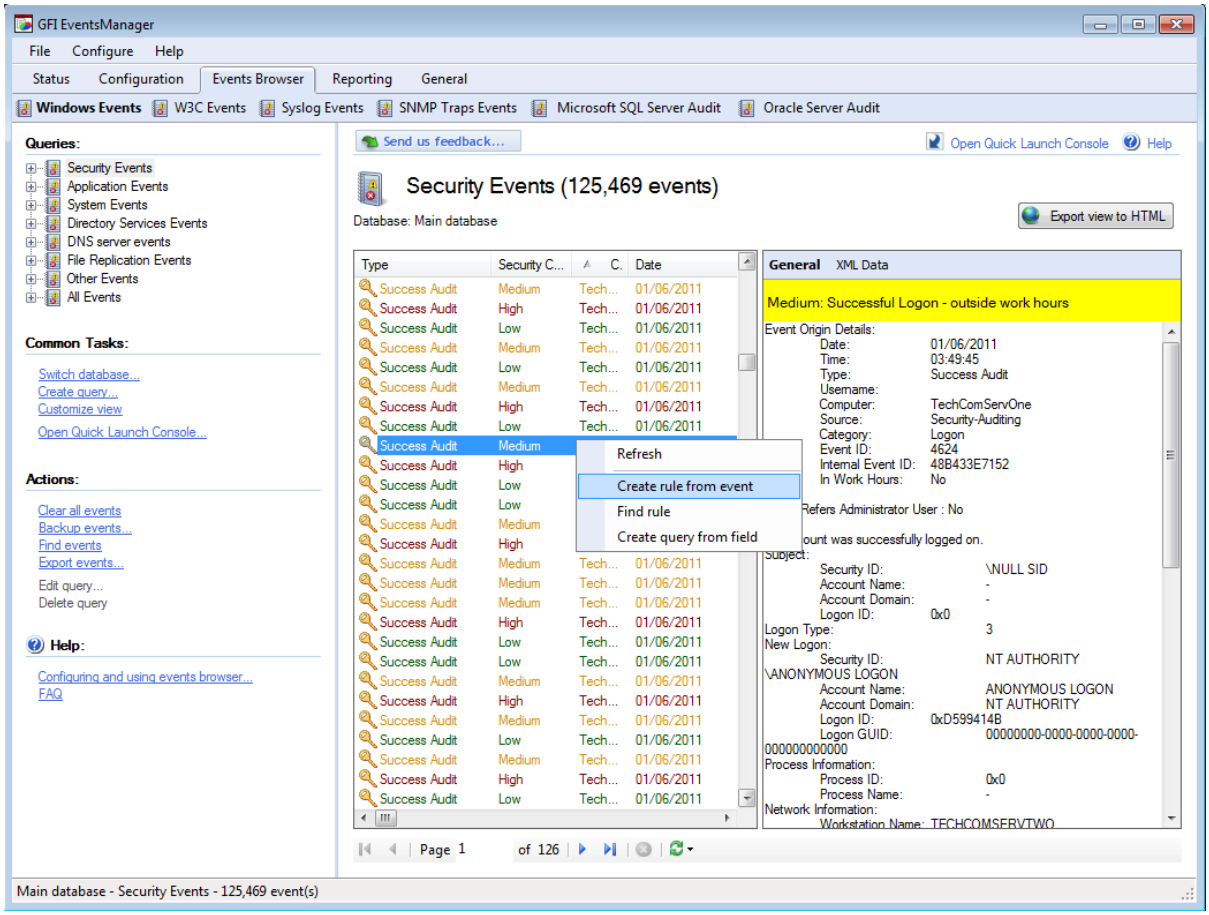
GFI EventsManager allows the creation of a new rule from an existing Windows Event.

Create new rule from event

To create a new rule from an existing Windows Event:

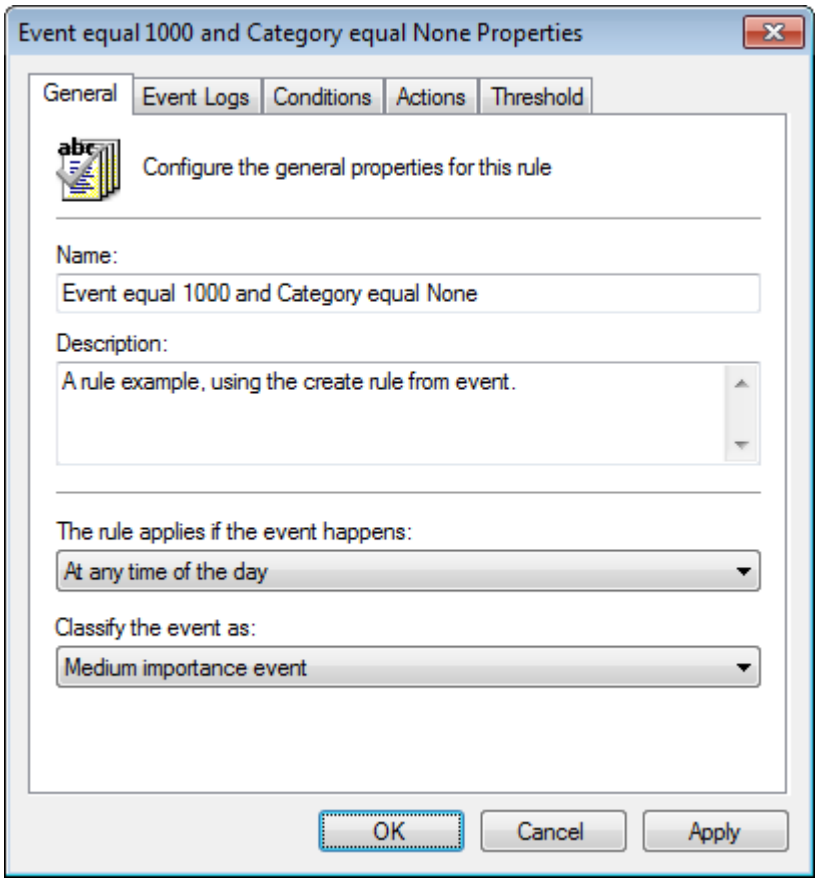
1. Select **Events Browser ► Windows Events**

2. Right click the event and select **Create rule from event**.

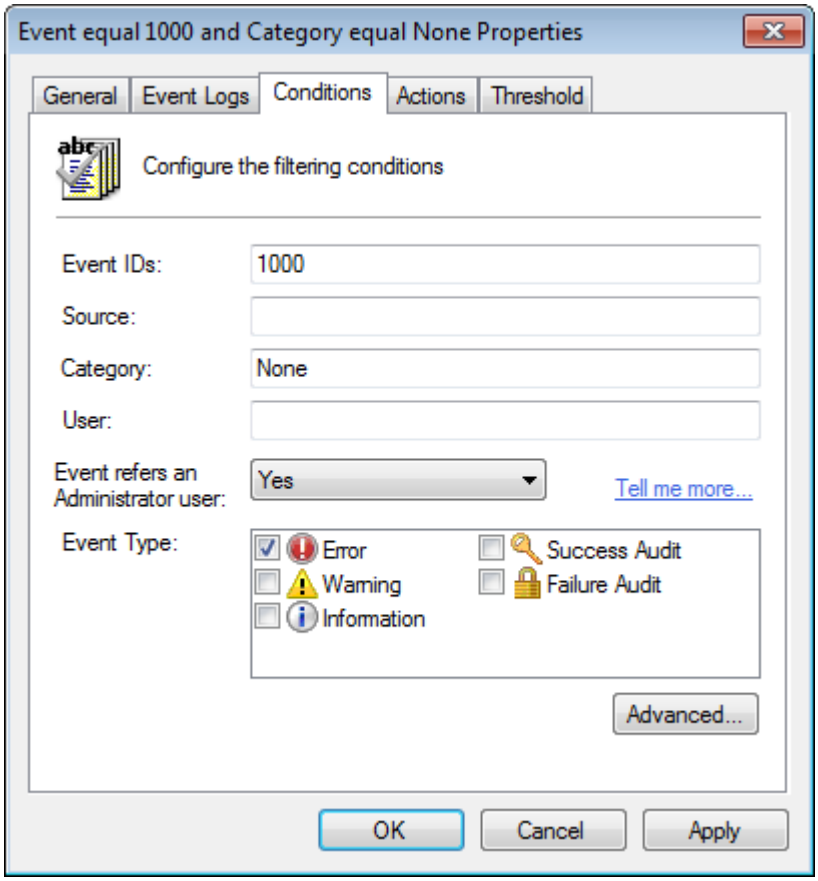


Screenshot 125 - Create rule from event

3. In the rule properties dialog box, key-in a valid name and an optional description.



Screenshot 126 - New Rule dialog



Screenshot 127 -Updated conditions for the selected rule

4. Select the **Conditions** tab and update the fields as required.

Conditions such as Event ID, Source and Category are updated automatically from the selected Windows event.

5. Select the **Actions** tab and configure the type of action to perform when the event occurs. You can choose to ignore the event, trigger the default action, or customize alerts.

6. Click **Ok** to save and close the rule dialog.

8.3.7 View or Edit a custom rule

To view or edit the new rule created:

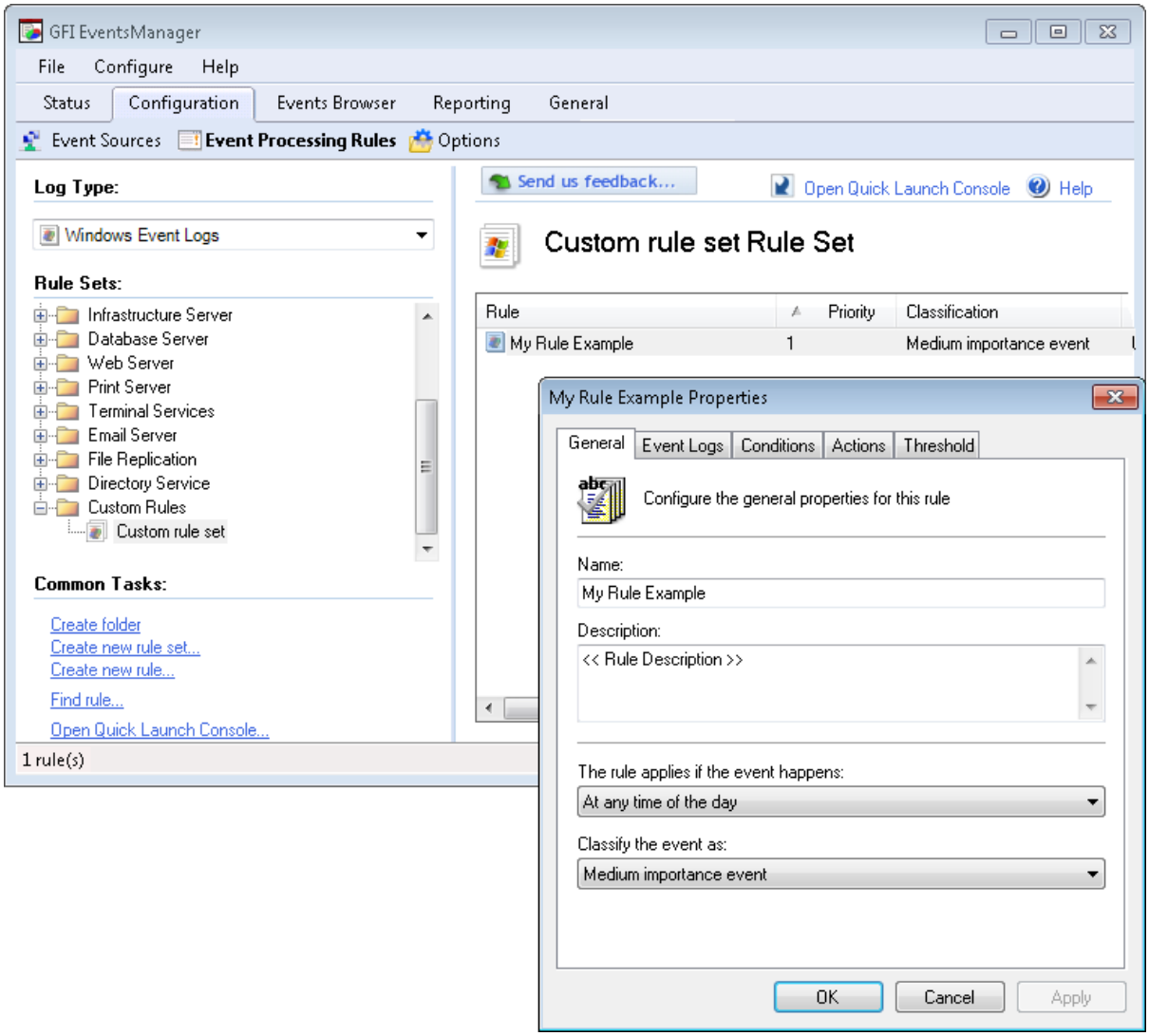
1. Click **Configuration** tab, select **Log Type**.

2. From the **Rule Sets** list, locate and click the **Custom Rules** folder.

3. Click **Custom rule set** rule and in the right panel locate the new rule created.

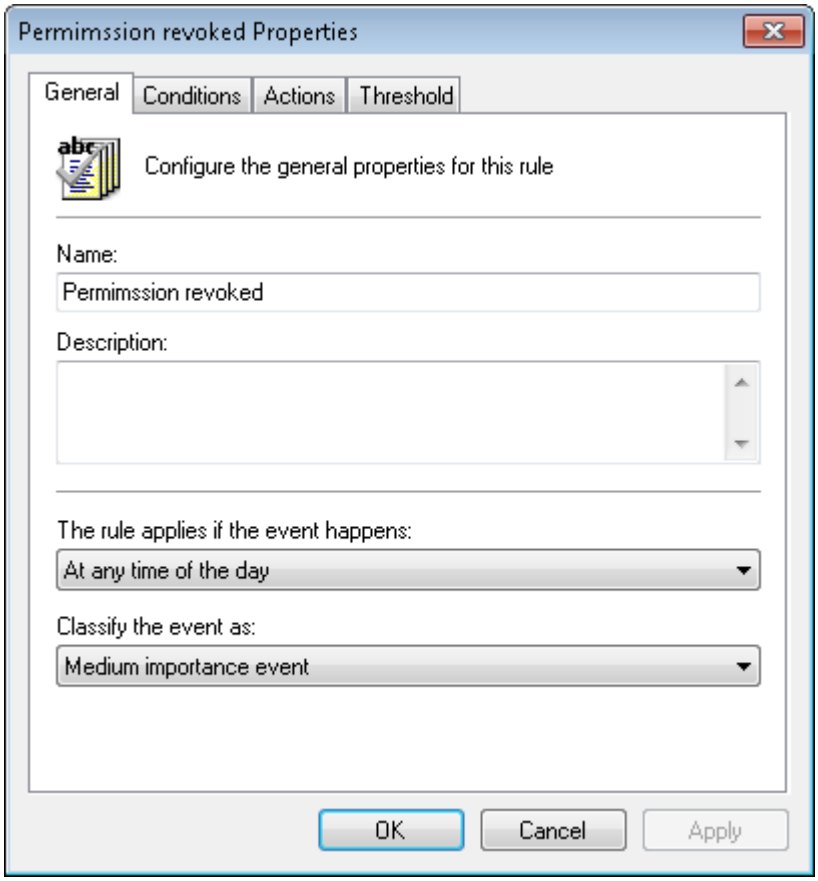
4. Right click the rule to:

- Disable
- Delete
- Increase or decrease priority
- Edit properties.



Screenshot 128 - Edit an existing custom rule

8.3.8 Changing the configuration settings of a rule



Screenshot 129 - Log processing rule properties

To edit the property settings of an event processing rule:

1. Right-click on the rule and select **Properties**.

2. Use the tabs provided in the dialog to navigate the existing parameters and make the required changes. The tabs provided in the properties dialog include:

- **General** - Use this tab to configure the general properties of the rule including the rule name and rule classification.
- **Logs** - This tab is available only for W3C log rules. Use this tab to specify the W3C logs for which this rule applies.
- **Event Logs** - This tab is available only for Windows Event Log rules only. Use this tab to specify which events will be processed by this rule.
- **Conditions** - Use this tab to configure event filtering conditions.
- **Actions** - Use this tab to configure alerts and actions triggered by this rule.
- **Threshold** - Use this tab to configure the event threshold value i.e. the number of times that an event must be detected prior to triggering alerts and remedial actions. This helps reducing false positives triggered by noise (repeated events) in your event logs.

8.4 Advanced event filtering parameters

GFI EventsManager allows systems administrators to set up advanced event filtering parameters. These options are available only for Windows Events and Syslogs.

8.4.1 Windows events conditions

The **Event IDs:** field allows systems administrators to setup parameters described in Table 28 below.

Table 28 - Parameters available in the Event ID field

PARAMETER TYPE	EXAMPLE
Single events	Event IDs: 575
List of events	Event IDs: 550, 570
Range of events	Event IDs: 575-600
Combination of events	Event IDs: 550, 570, 575-600

The **Source**, **Category** and **User** fields allow systems administrators to setup parameters described in Table 29 below.

Table 29 - Parameters available in the Source, Category and User fields

PARAMETER TYPE	EXAMPLE
Single source name	Source: Userenv
List of sources	Source: Userenv, SceCli
Wildcards (% and *)	Source: S%t%

8.4.2 Syslog categories

The **Message** and **Process** fields allow systems administrators to setup parameters described in Table 30 below.

Table 30 - Parameters available in the Message and Process fields

PARAMETER TYPE	EXAMPLE
Single message	Message: session opened
List of messages	Message: session opened, session closed
Wildcards (% and *)	Message: %session opened%

8.4.3 Field operators

Field operators are used in advanced filtering. Filters process events based on the field operator and a value, configured by the user. Available field operators, include:

- **Equal to** - When the event field is equal to the value configured.
- **Not Equal to** - When the event field is not equal to the value configured.
- **Contains the text** -When the event field contains the value text.
- **Does not contain the text** - When the event field does contains the value text.
- **Like** - When the event field has similar text as the value text.
- **Value in set** - When the event field is equal to one of the values in a list.
- **Value not in set** - When the event field is not equal to one of the values in a list.

To create a list in the value field, enter all items separated by a semicolon ‘;’.

Screenshot 130 - Available field operators

9 Customizing alerts and actions

9.1 Introduction

During event processing, GFI EventsManager can automatically generate various actions whenever particular events are encountered. Supported actions include email alerts and event archiving.

You can specify alerts and actions to be triggered in two ways:

1. By configuring a set of 'Default classification actions '.

2. By creating or customizing rules and rule-sets.

Default classification actions

Through the configuration parameters provided in the default classification actions, you can trigger alerts and actions based only on event classification. For example, default classification parameters can be configured to trigger email alerts for all classified events (critical, high, medium and low) but archive only critical events.

Generating actions through event processing rules

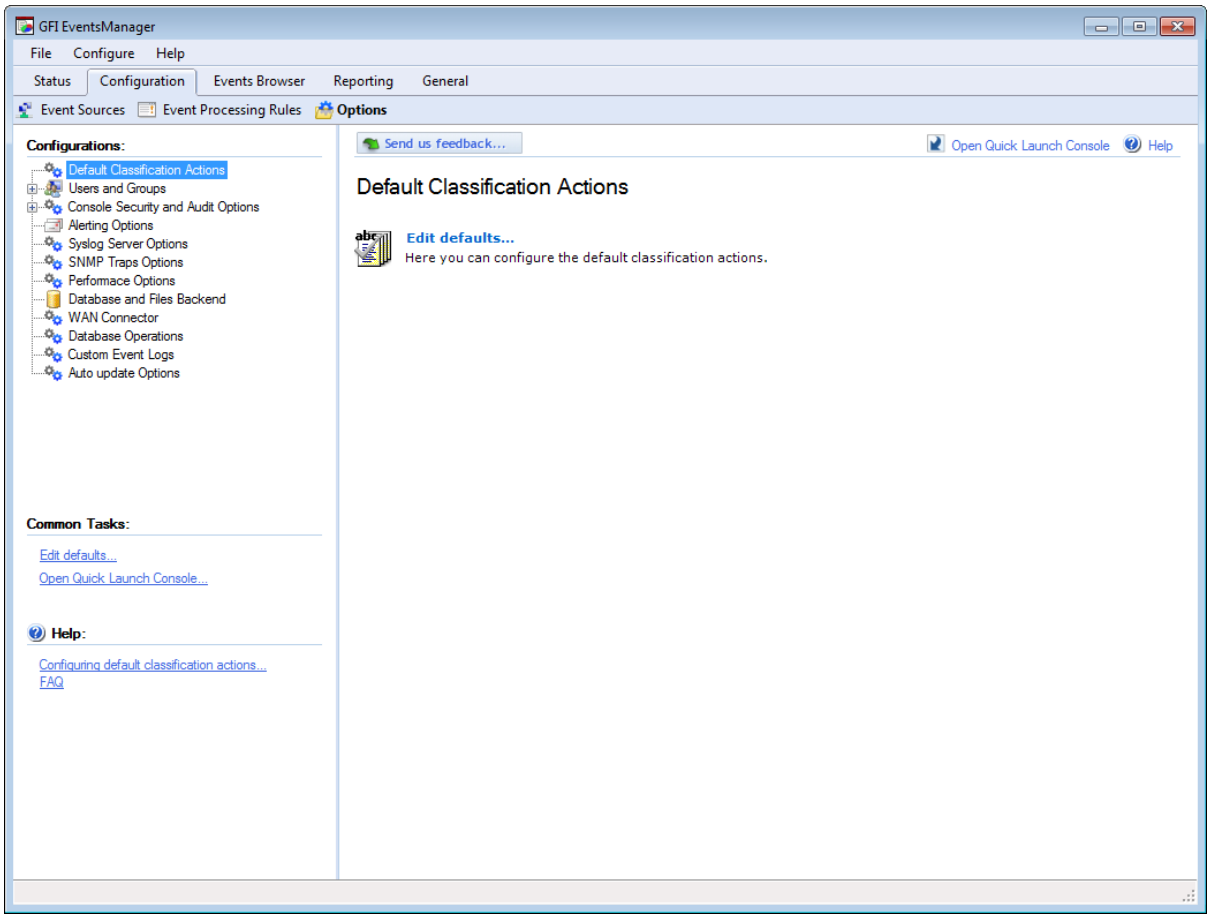
Rules allow you to configure actions on a more granular level. Rules allow you to configure and trigger actions whenever an event fits one or more specific conditions. For example, you can create a rule which archives only events having event ID 231, regardless their classification.

Supported actions

GFI EventsManager supports the following actions:

- **Archive the event** - Archives the classified event into the GFI EventsManager database back-end.
- **Send e-mail, SMS, network or SNMP notifications to** - Sends email, SMS network or SNMP alerts to specific recipients.
- **Run File** - Runs an executable file. Files that can be executed include VBScripts (.VBS), Batch files (.BAT) or another executable type of file (.EXE). You can also specify any command-line parameters to pass on to the executable file.

9.2 Configuring default classification actions

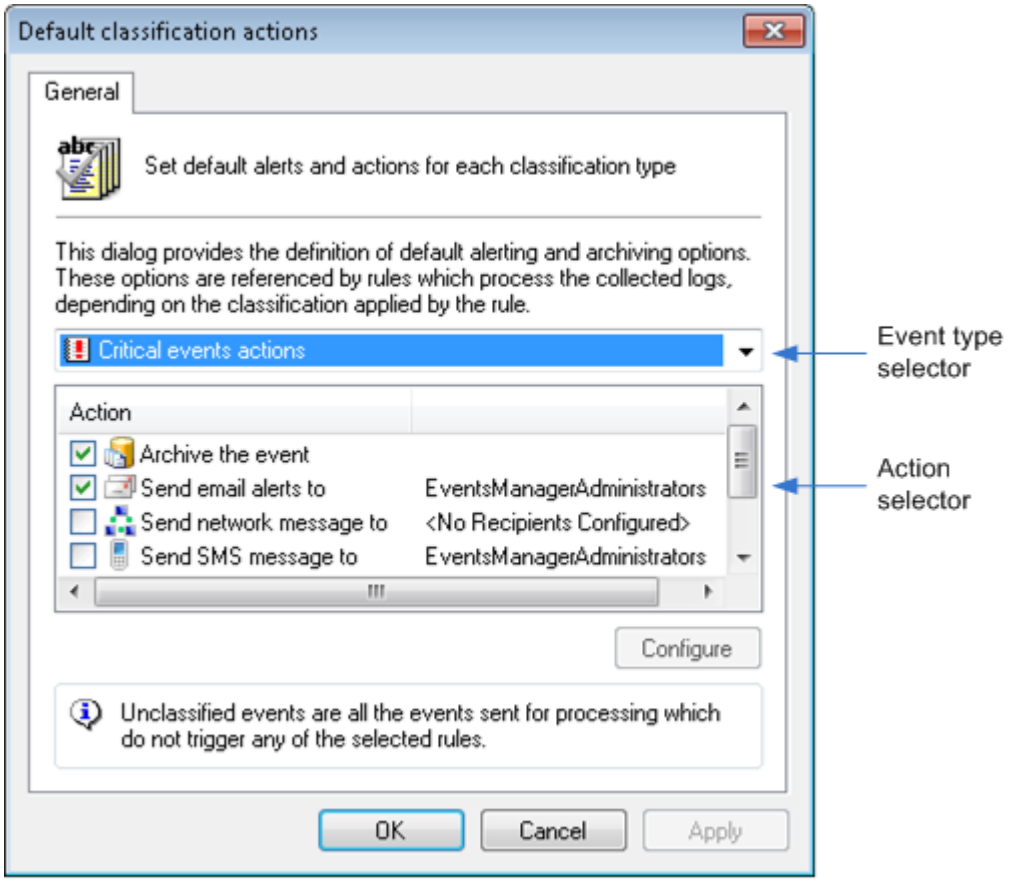


Screenshot 131 - Configuring default classification actions

To configure default classification actions:

1. Click the **Configuration** tab and select **Options**.

2. From **Configurations**, right-click on the **Default Classification Actions** node and select **Edit defaults…**.


Default classification actions
General
Set default alerts and actions for each classification type
This dialog provides the definition of default alerting and archiving options. These options are referenced by rules which process the collected logs, depending on the classification applied by the rule.
Critical events actions
Action
Archive the event
Send email alerts to
EventsManagerAdministrators
Send network message to
<No Recipients Configured>
Send SMS message to
EventsManagerAdministrators
Configure
Unclassified events are all the events sent for processing which do not trigger any of the selected rules.
OK
Cancel
Apply
Event type selector
Action selector

Screenshot 132 - Default classification actions screen

3. From the provided drop-down, select the event classification to be configured.

4. From **Action** list, select actions to be triggered for the selected classification.

5. Click **Configure to** specify any parameters required by the selected action.

Be aware that assigning actions on events classified as low might generate:

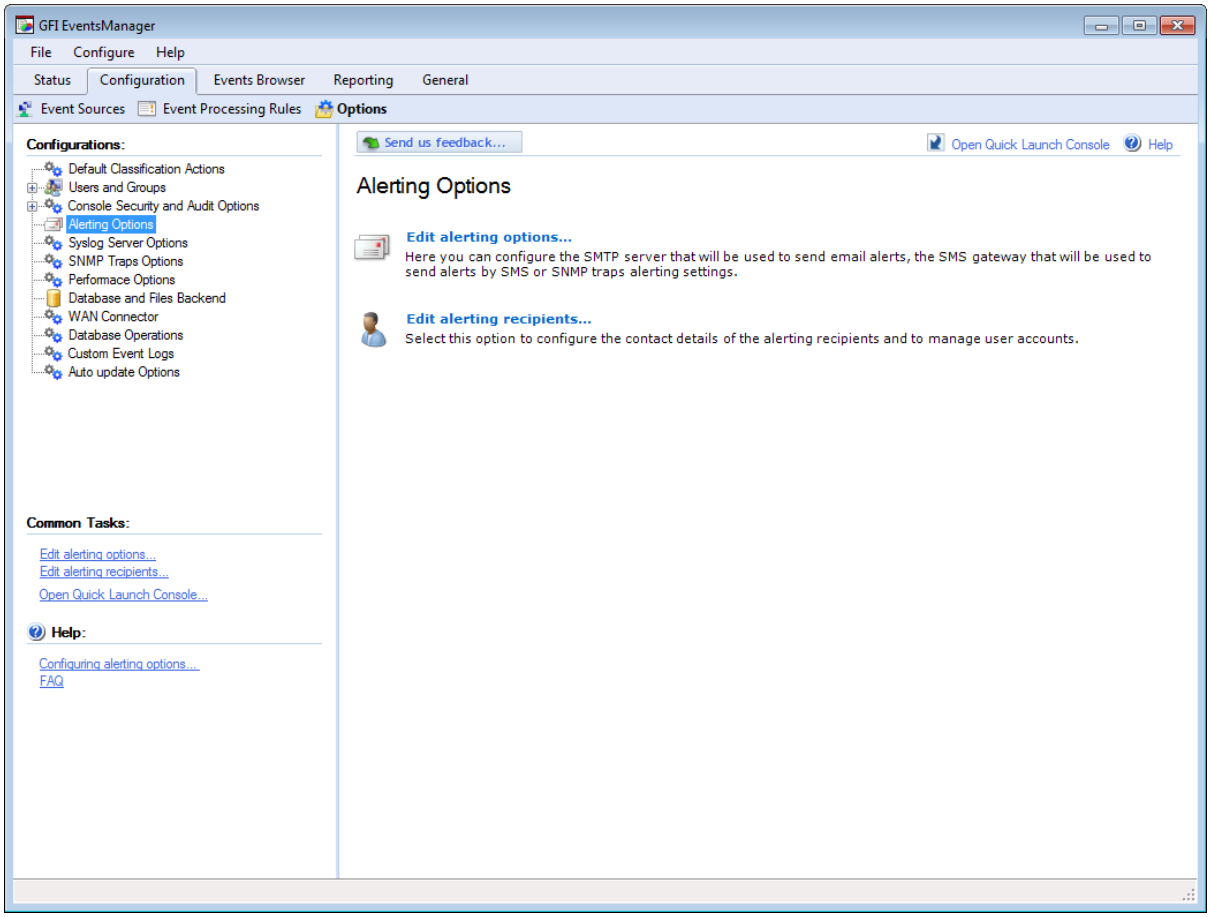
» A lot of network traffic (especially if email, SMS, network or SNMP alerts are being generated)

» A high volume of database data/transactions if events are being archived.

9.3 Configuring alerting options

GFI EventsManager will automatically send out email, network, SMS or SNMP alerts whenever particular events are discovered. Supported alerting methods require the configuration of a set of general alerting parameters that are network specific. For example, to send email alerts, GFI EventsManager must know which SMTP Server will be used to propagate email alerts.

While GFI EventsManager issues alerts automatically whenever particular alerts are discovered, it is important to configure the email address/es of the recipients of such alerts. By default, GFI EventsManager will automatically create the **EventsManagerAdministrator** account to which you can assign an email address. For more information on how to configure administrator contact details refer to Configuring the administrator account section in this manual.



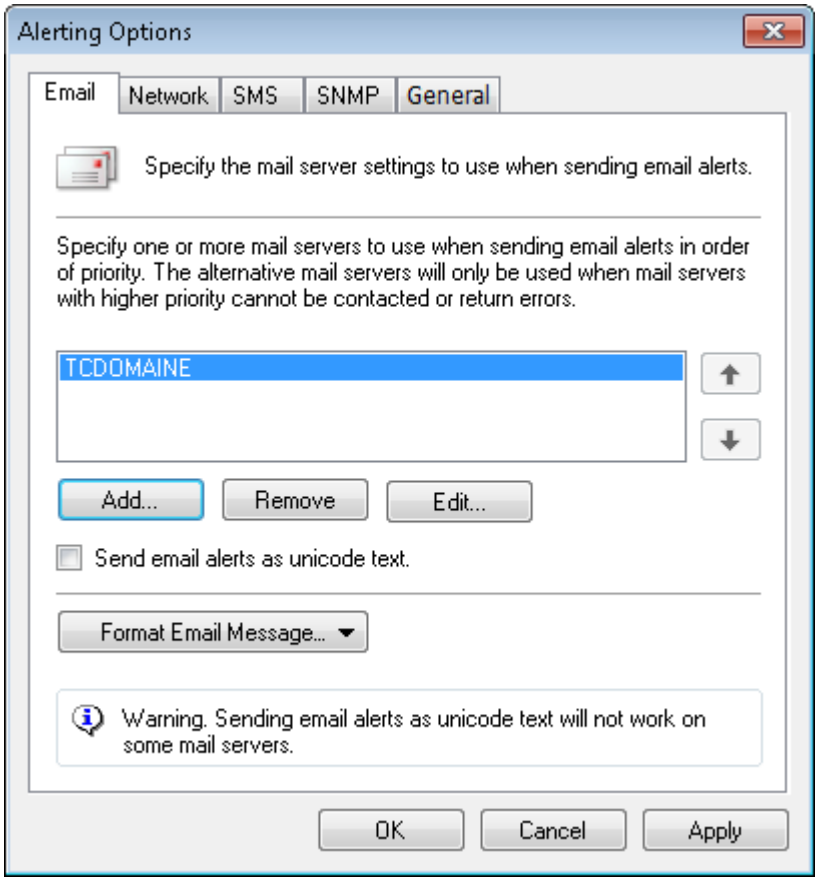
Screenshot 133 - Configuring alerting options

To configure alerts:

1. Click **Configuration** tab and select **Options**.

2. From **Configurations**, right-click on the **Alerting Options** node and select **Edit alerting options…** option.

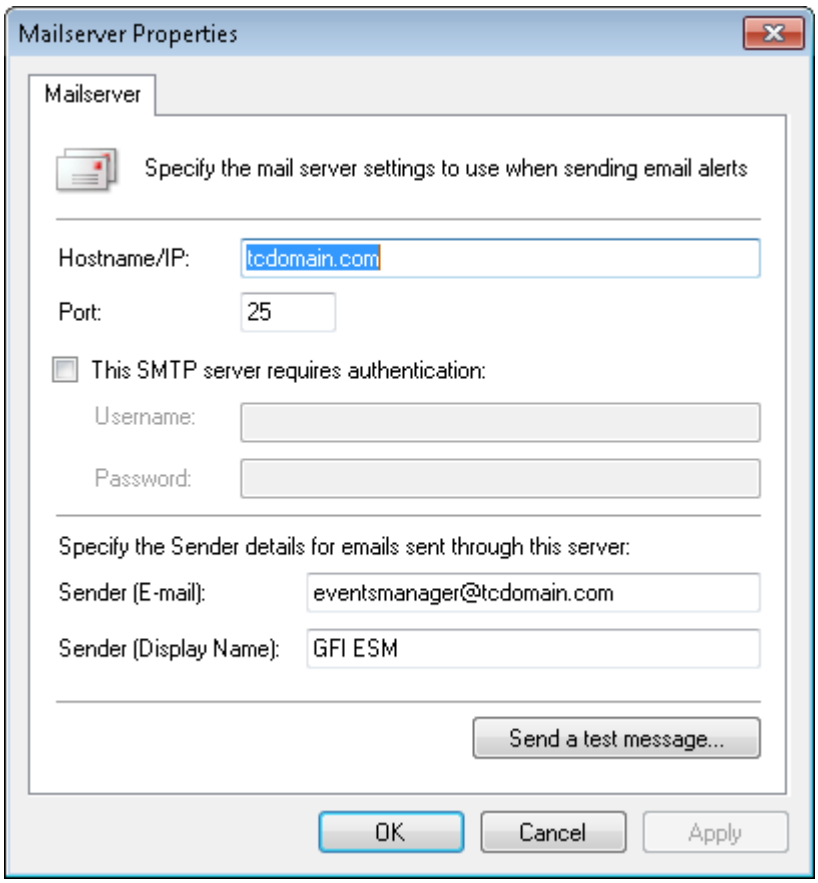
Select **Edit alert recipients** to configure the contact details of the alerting recipients and to manage user accounts. For more information, refer to Manage user accounts section in this manual.


Alerting Options
Email
Network
SMS
SNMP
General
Specify the mail server settings to use when sending email alerts.
Specify one or more mail servers to use when sending email alerts in order of priority. The alternative mail servers will only be used when mail servers with higher priority cannot be contacted or return errors.
TCDOMAINE
Add...
Remove
Edit...
Send email alerts as unicode text.
Format Email Message...
Warning. Sending email alerts as unicode text will not work on some mail servers.
OK
Cancel
Apply

Screenshot 134 - Alerting options dialog

This will launch the **Alerting Options** dialog. Use the **Email**, **Network**, **SMS** and **SNMP** tabs provided in this dialog to configure the default alerting settings. More information on how to configure these settings is provided below.

9.3.1 Configuring email alerts



Screenshot 135- Mail server properties dialog box

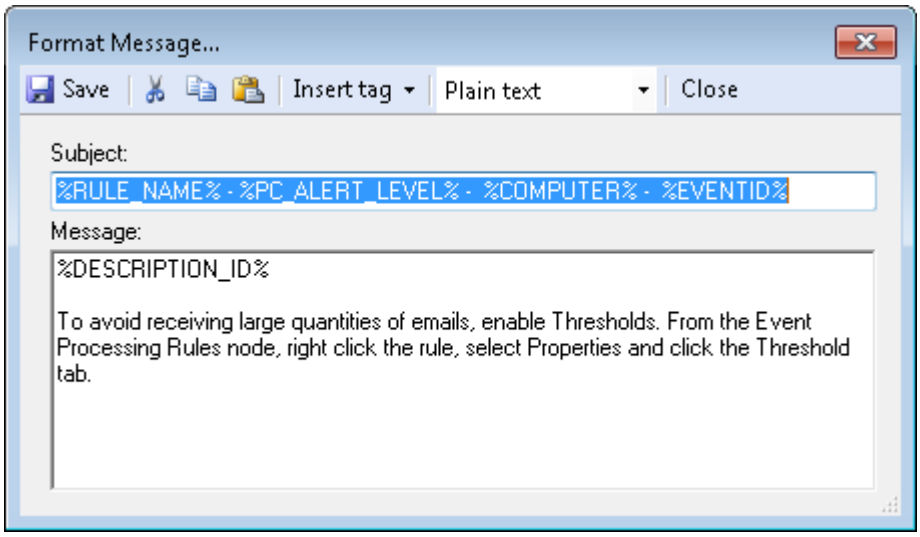
To configure email alerts:

1. From **Email** tab, click **Add**.

2. Specify the name/IP of your mail server. If required specify also the mail server authentication details.

3. Specify the email address and display name that will be used when sending email alerts.

4. To customize the email text message, click **Format Email Message…**.

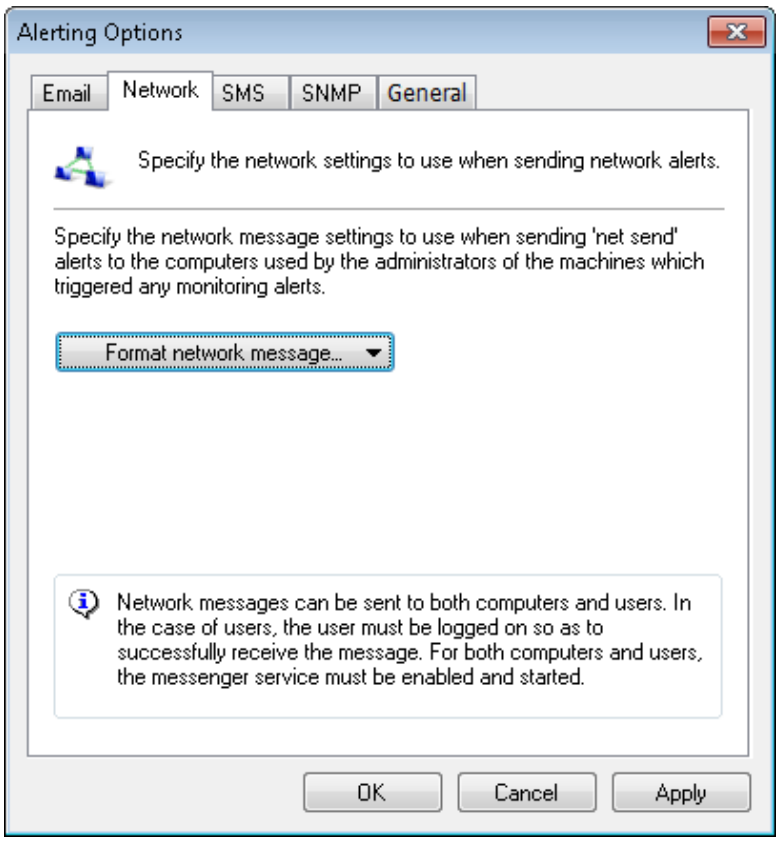

Format Message...
Save
Insert tag
Plain text
Close
Subject:
%RULE_NAME% - %PC_ALERT_LEVEL% - %COMPUTER% - %EVENTID%
Message:
%DESCRIPTION_ID%
To avoid receiving large quantities of emails, enable Thresholds. From the Event Processing Rules node, right click the rule, select Properties and click the Threshold tab.

Screenshot 136- Format mail message

5. If required, click on the **Network**, **SMS** or **SNMP** tabs to configure the respective parameters.

6. Click **OK** to finalize settings.

9.3.2 Configuring network alerts

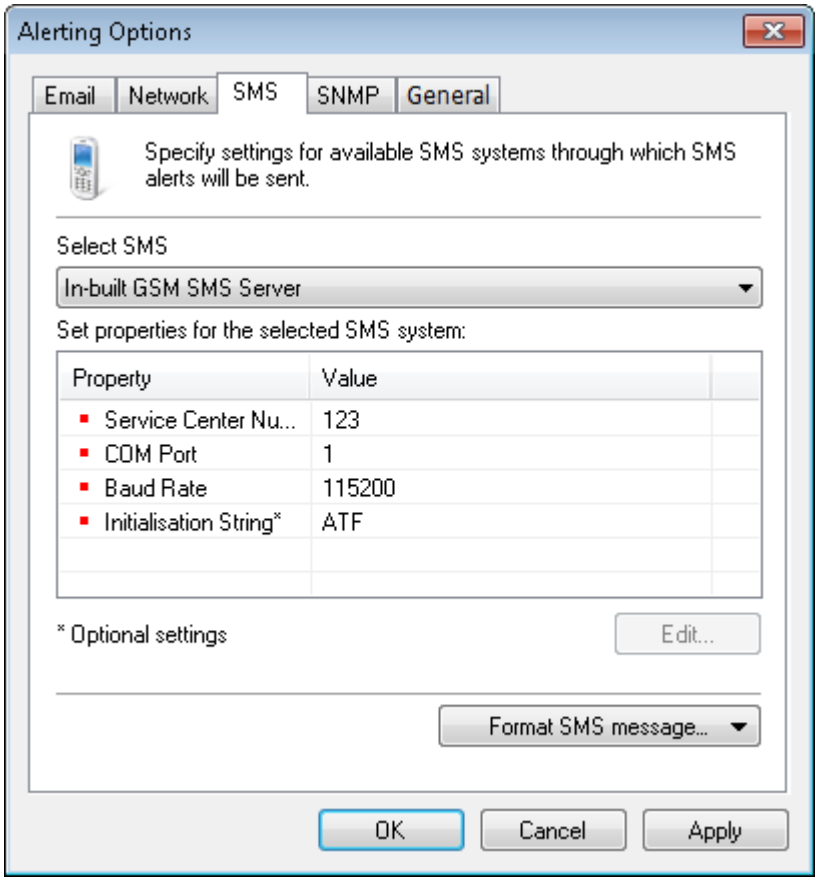

Alerting Options
Email
Network
SMS
SNMP
General
Specify the network settings to use when sending network alerts.
Specify the network message settings to use when sending 'net send' alerts to the computers used by the administrators of the machines which triggered any monitoring alerts.
Format network message...
Network messages can be sent to both computers and users. In the case of users, the user must be logged on so as to successfully receive the message. For both computers and users, the messenger service must be enabled and started.
OK
Cancel
Apply

Screenshot 137 - Alerting Options: Network dialog box

1. Access **Network** tab

2. Click **Format network message…** to customize the network message.

9.3.3 Configuring SMS alerts



Screenshot 138 - Alerting Options: SMS dialog box

SMS alerts can be sent using various methods. Supported methods include GFI FAXmaker SMS gateway and Clickatell Email to SMS service gateway. To configure which method will be used to convey SMS alerts:

1. Access **SMS** tab

2. From the **Select SMS**, select the SMS system through which SMS notification will be sent.

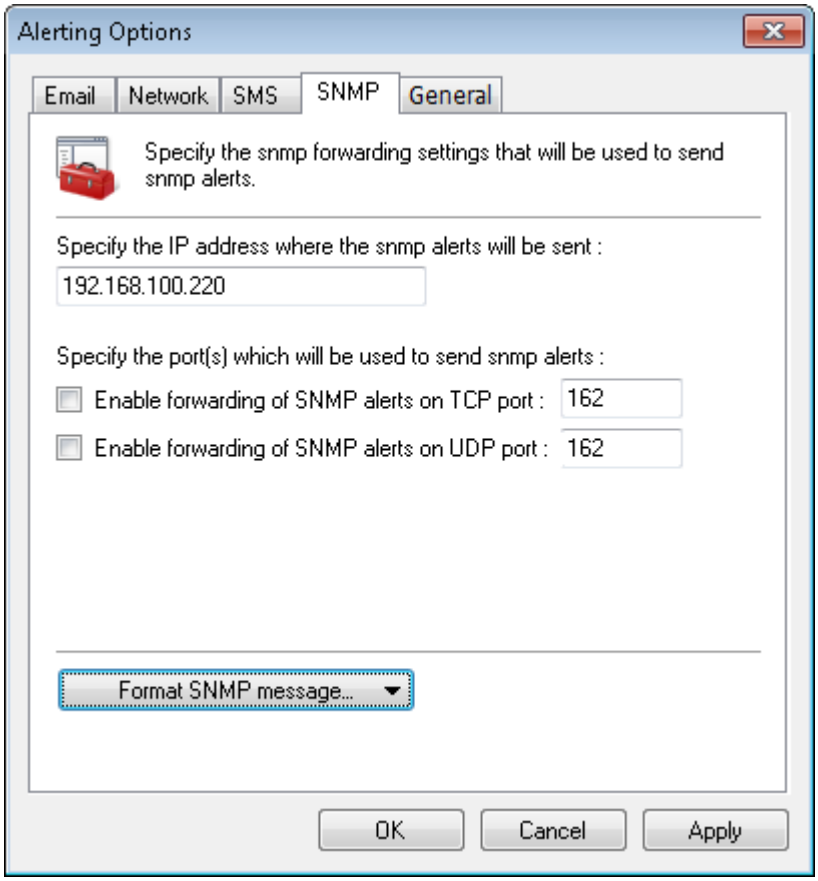
3. Select the property to be configured from the list provided and click **Edit…**

4. Repeat until all required properties have been configured.

5. To customize the SMS alert message, click **Format SMS message….**

6. Click on **OK** to finalize settings.

9.3.4 Configuring SNMP alerts

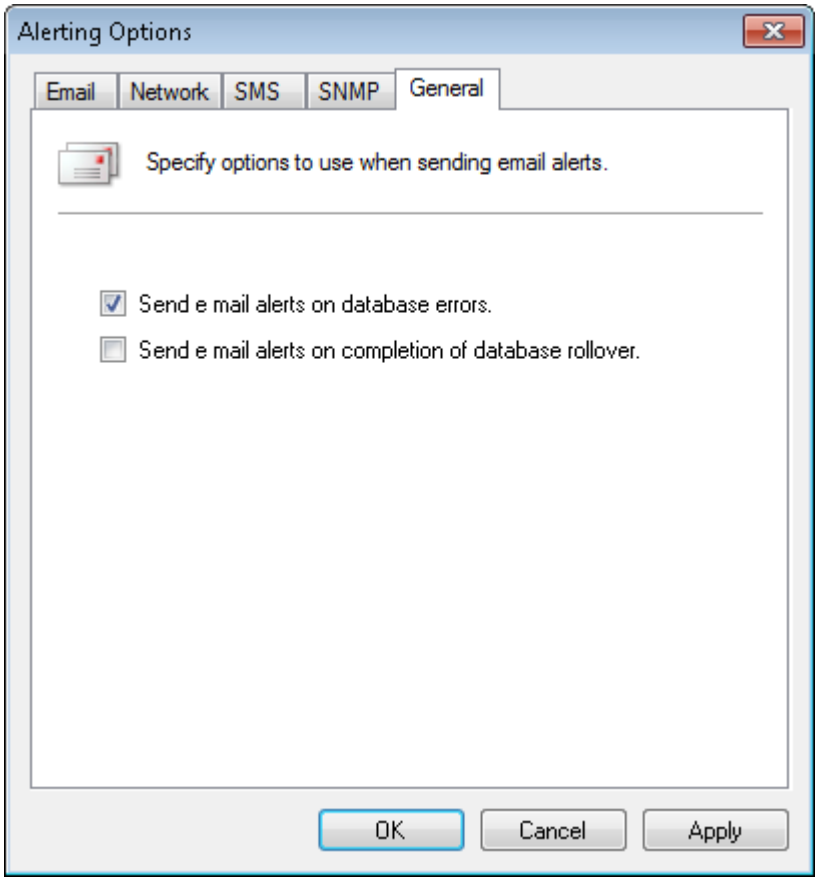


Screenshot 139 - Alerting Options: SNMP dialog box

To configure SNMP alerts:

1. Access **SNMP** tab
2. Specify the IP address where SNMP alerts will be sent.
3. (Optional) specify the port/s that will be used to send the SNMP alerts.
4. To customize the email text message, click **Format SNMP Message…**.
5. Click **OK** to finalize settings.

9.3.5 Configuring generic alerts



Screenshot 140 - Alerting Options: SNMP dialog box

To configure database alerts:

1. Click **General** tab.

2. Select options described in Table 31 below:

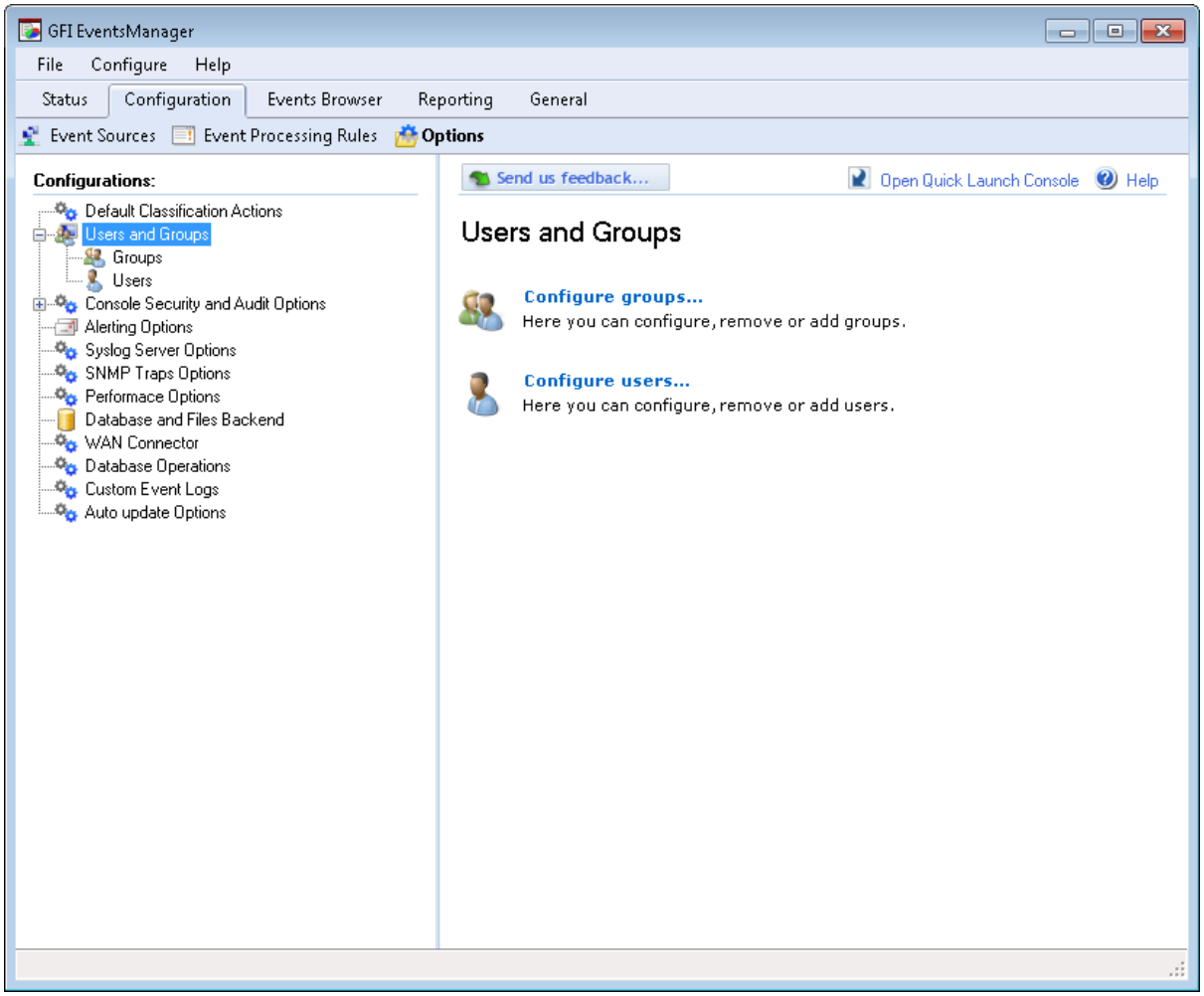
Table 31 - Database alerts options

OPTION	DESCRIPTION
Send email alerts on database errors	Email alerts are sent upon database errors such as backup failure, data corruption, size exceeds maximum size specified and other database operation errors.
Send email alerts on completion of database rollover	Email alerts are sent when a database rollover is complete.

3. Click **OK** to finalize settings.

10 Configuring users and groups

10.1 Introduction



Screenshot 141 - Configuring users and group's node

Use the Users and Groups node to assign different console access privileges to GFI EventsManager users. Through this node users and groups can be configured, amended or deleted. Working hours and alerts can also be configured and assigned to groups.

Use the users and groups node also to assign users administrative privileges. These privileges allow users to browse events as well as modify GFI EventsManager configuration settings.

10.2 Manage user accounts

10.2.1 Configuring the administrator account

GFI EventsManager will automatically create the 'EventsManagerAdministrator account. However, you must still configure details such as the email address and mobile number of the GFI EventsManager administrator.

GFI EventsManager requires a valid administrator email address in order to distribute automatic alerts when particular events are discovered.

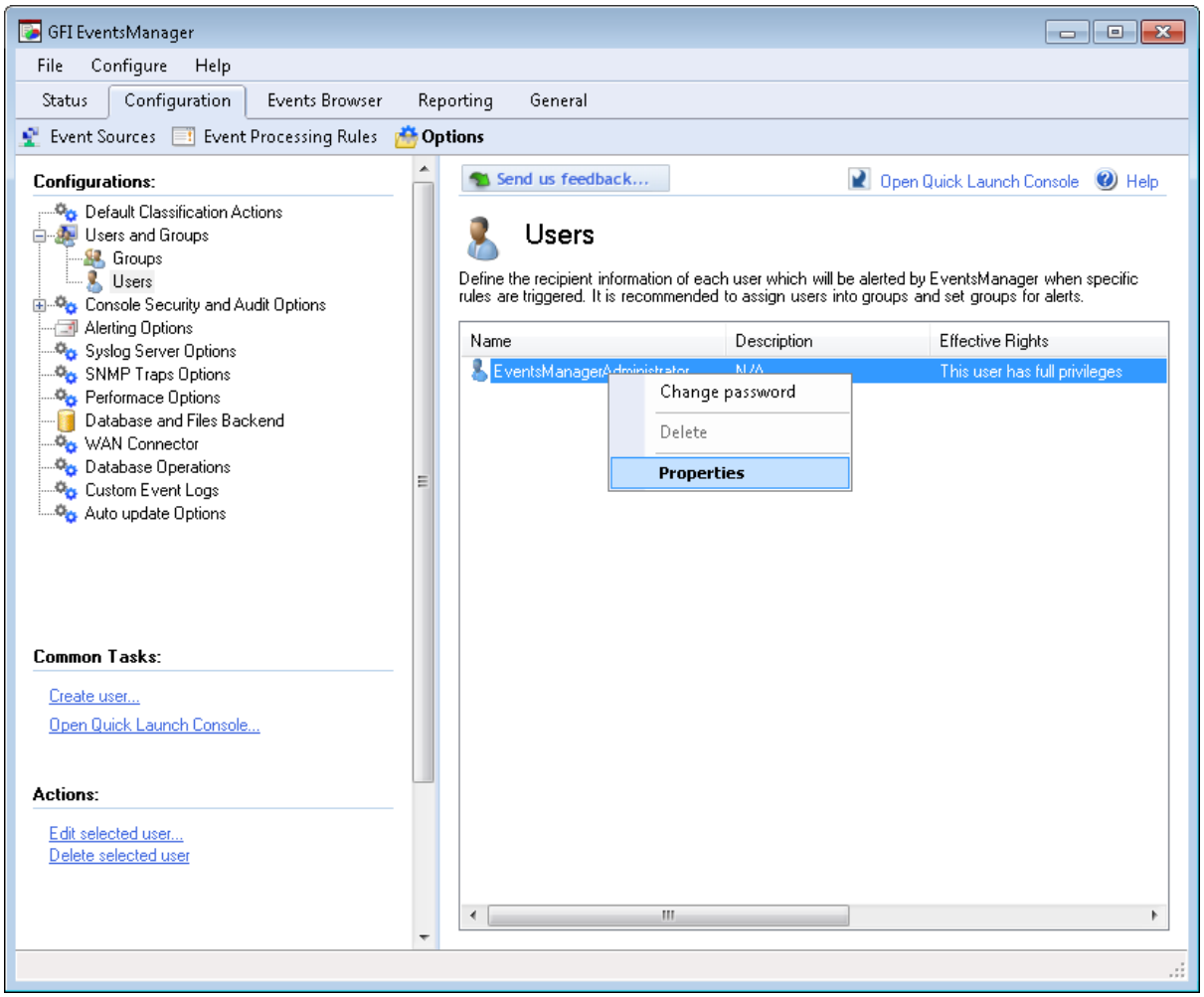
For every user (including the administrator), you can configure the following parameters:

» Contact details including email address and phone number

» The typical working hours

» The type of alert to send during and outside working hours

» The notification group to which the user belongs.



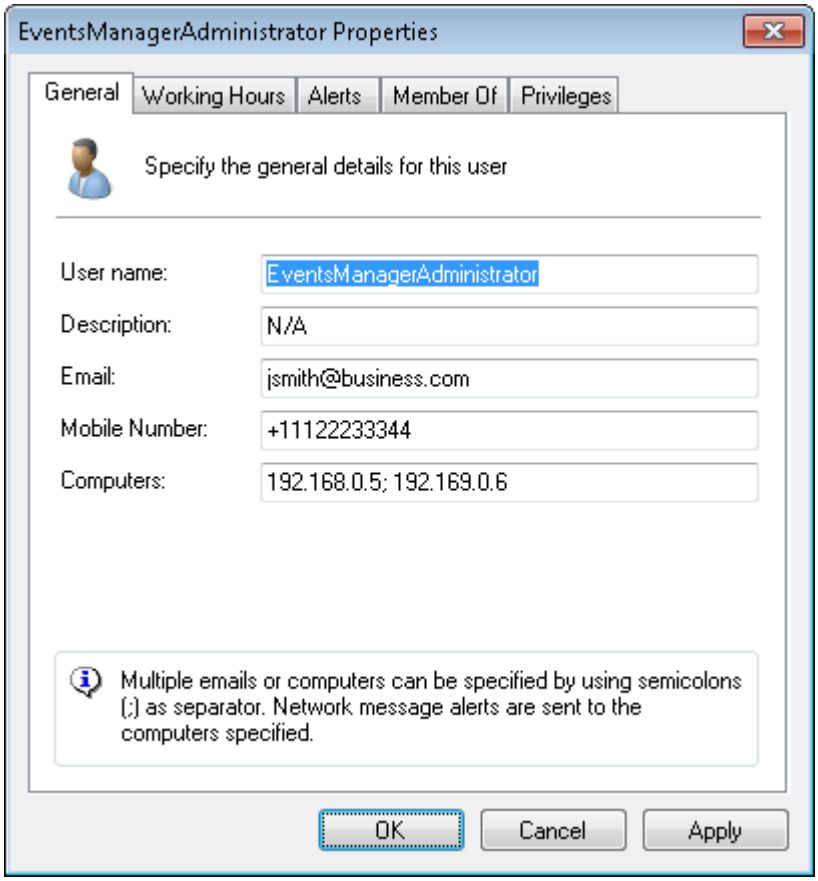
Screenshot 142 - Configuring the default EventsManagerAdministrator account

To configure the GFI EventsManagerAdministrator account:

1. Click **Configuration** tab and select **Options**.

2. Expand the **Users and Groups** node.

3. Click **Users** sub-node and in the right pane right click on the **EventsManagerAdministrator** account and select **Properties**.



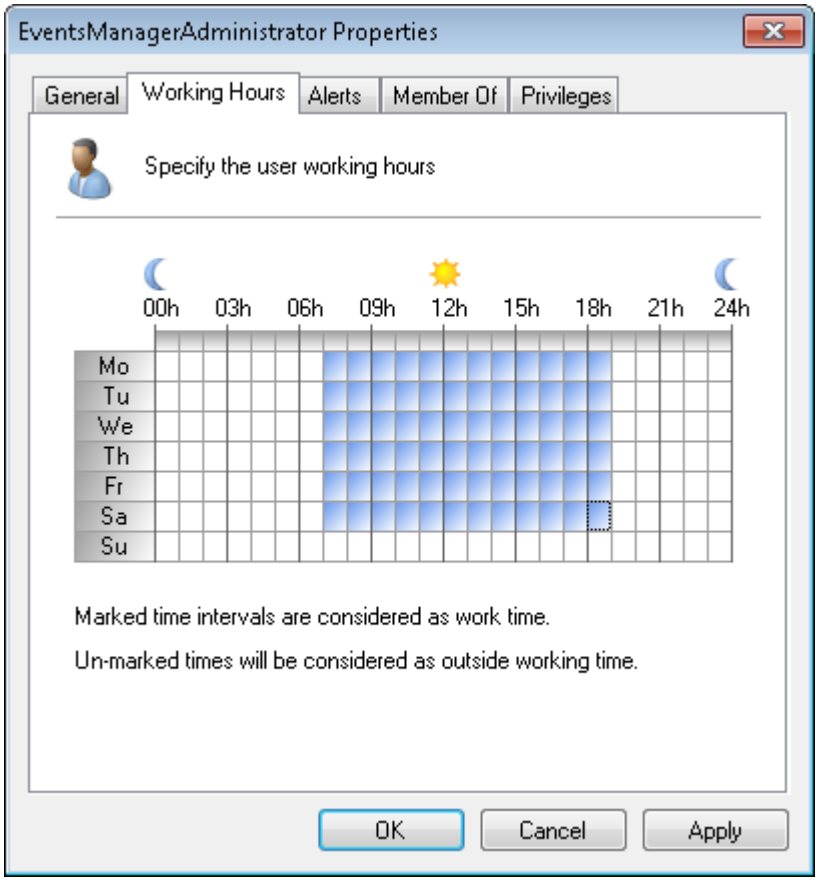
Screenshot 143 - EventsManager Administrator properties

Configuring the account sequence is as follows:

1. Specify the contact details such as email address, and mobile number as required.

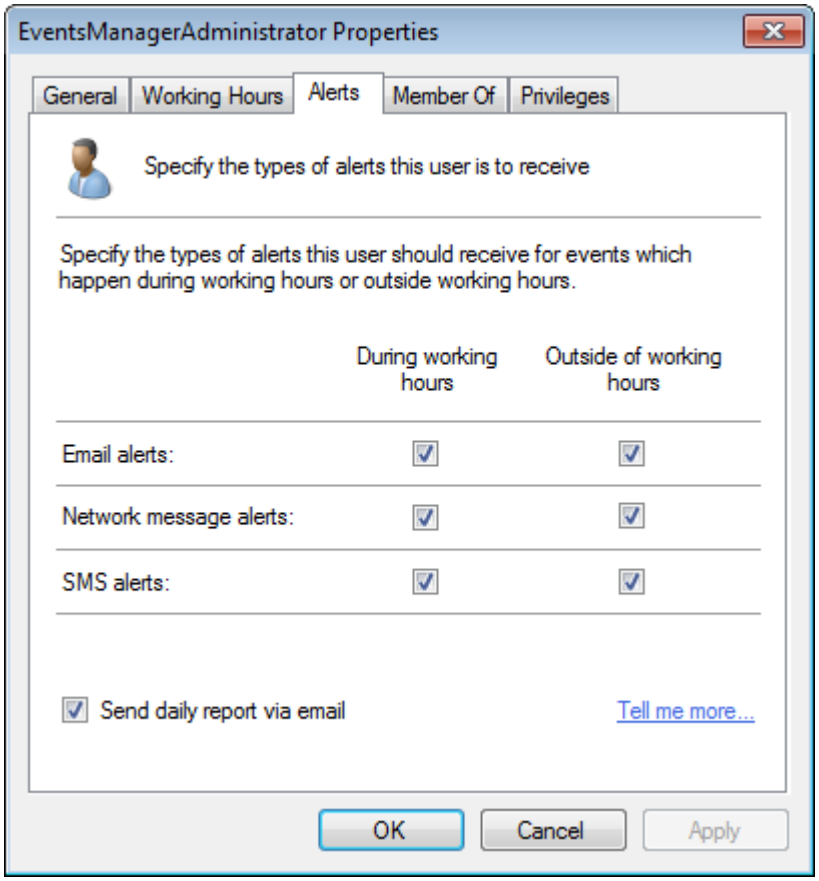
2. Specify the computers on which network alerts addressed to the administrator will be sent.

3. Click **Working Hours** tab.



Screenshot 144 - Configuring the typical working hours of an alert recipient

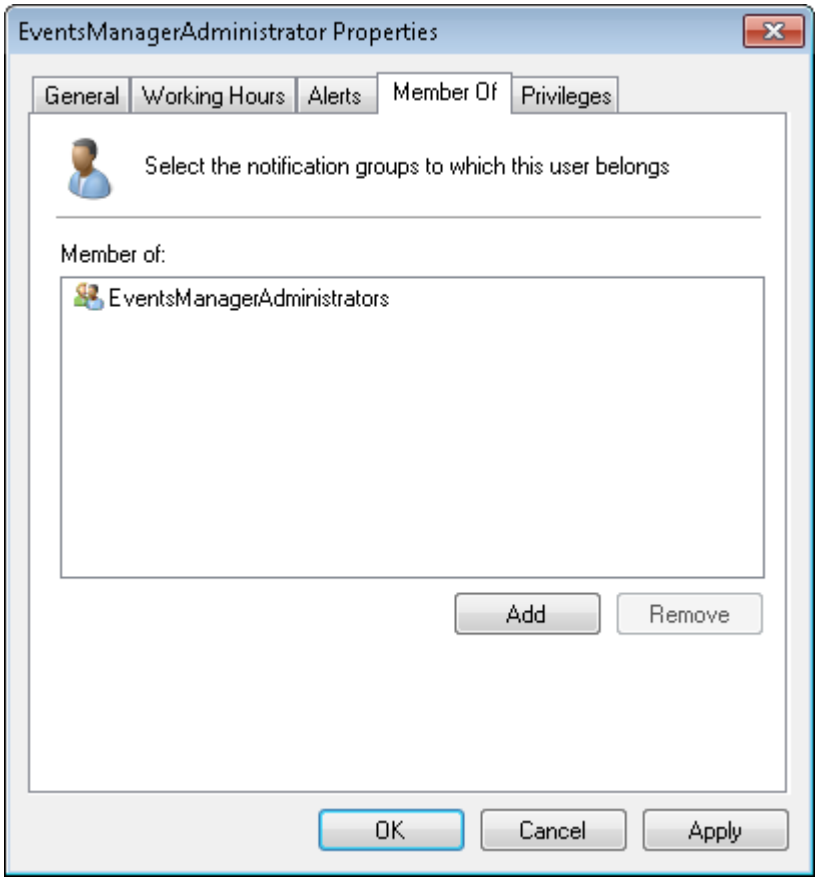
4. Select the typical working hours of the administrator/user.



Screenshot 145 - Selecting alerts to be sent during and outside working hours

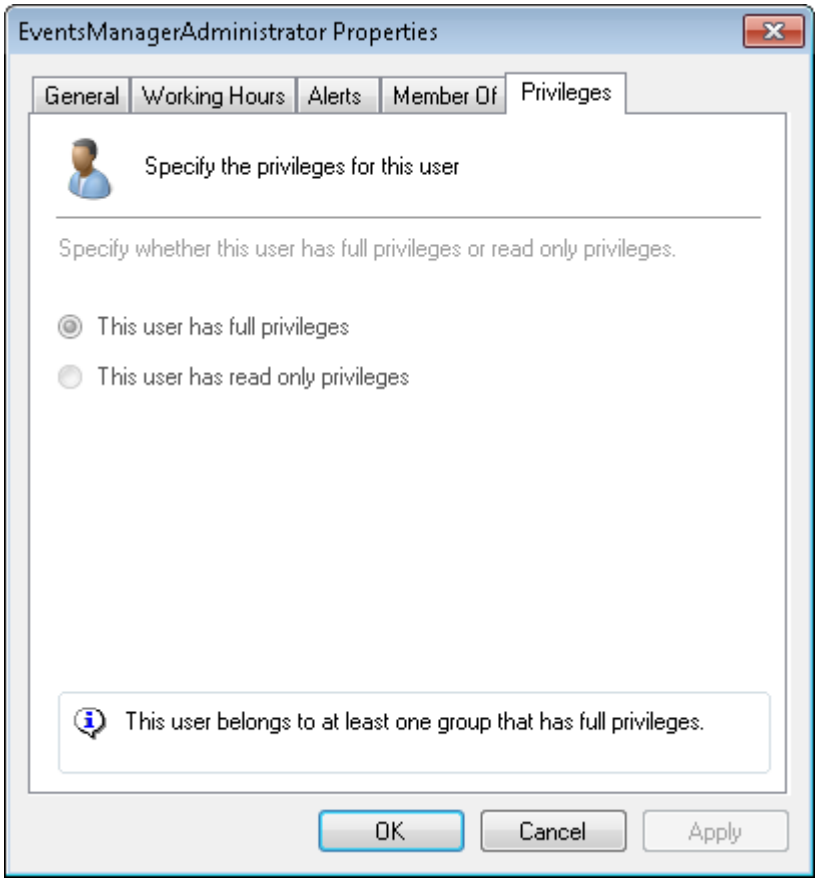
5. Click **Alerts** tab and select which alerts will be sent during and outside working hours.

6. (Optional) Select **Send daily report via email** to send a summary of the most important events collected and processed by GFI EventsManager by email.



Screenshot 146 - Notification groups to which a user belongs

7. Click **Member Of** tab and select the notification groups to which the user belongs. By default the administrator is a member of the 'EventsManagerAdministrators' notification group.



Screenshot 147 - Configuring GFI EventsManager administrator privileges

8. Click the **Privileges** to modify the user privileges on GFI EventsManager. By default the 'EventsManagerAdministrator' account has full privileges.

9. Click **OK** button to finalize your settings.

10.2.2 Create user accounts

GFI EventsManager allows you to create a custom list of users which you can organize into groups to speed up administrative tasks.

To create a new user:

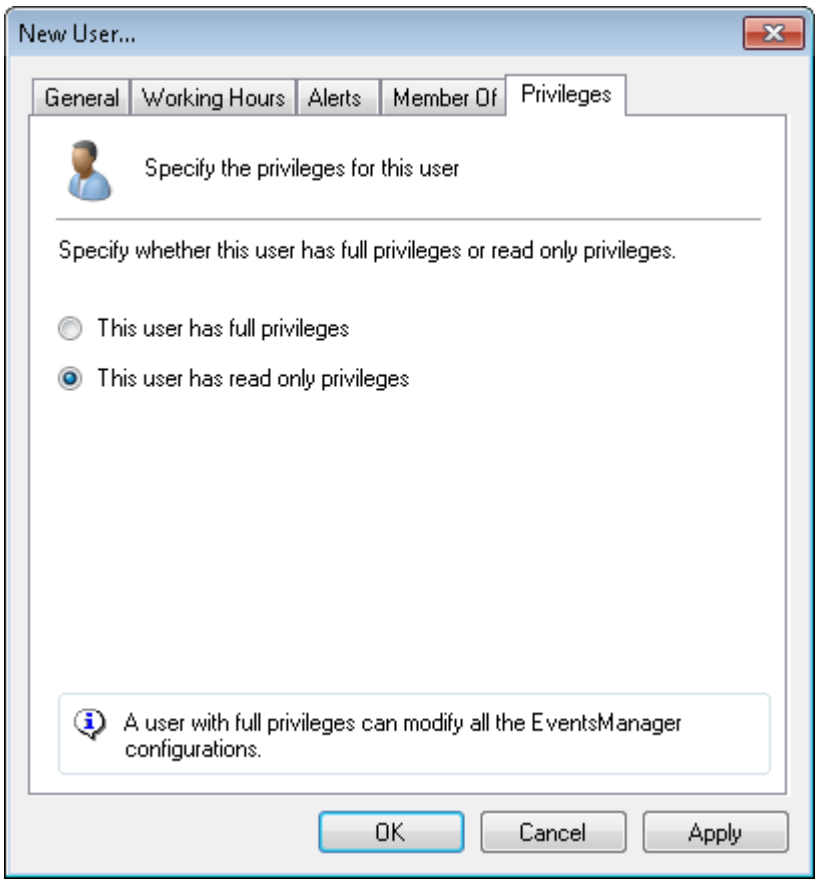
1. Click **Configuration** tab and select **Options**.

2. Expand the **Users and Groups** node.

3. Right-click on the **Users** sub-node and select **Create user…**

4. Specify the parameters requested in the **General**, **Working Hours**, **Alerts Member of** and **Privileges** tabs.

For more information on how to fill in these tabs, refer to Configuring the administrator account section in this manual.



Screenshot 148 - GFI EventsManager new user privileges

5. Click **Privileges** tab and select user privileges accordingly. E.g. To assign administrative privileges to a user select the **This user has full privileges** option.

Users with administrative privileges can modify all GFI EventsManager configuration settings.

6. Click **OK** to finalize setup.

10.2.3 Changing user properties

To edit user properties:

1. From the left pane, click on the **Users** node.

2. Right-click on the user to edit and select **Properties**.

3. Make the required changes in the tabs available and click **OK** to finalize your settings.

For more information on how to fill in these tabs, refer to Configuring the administrator account section in this manual.

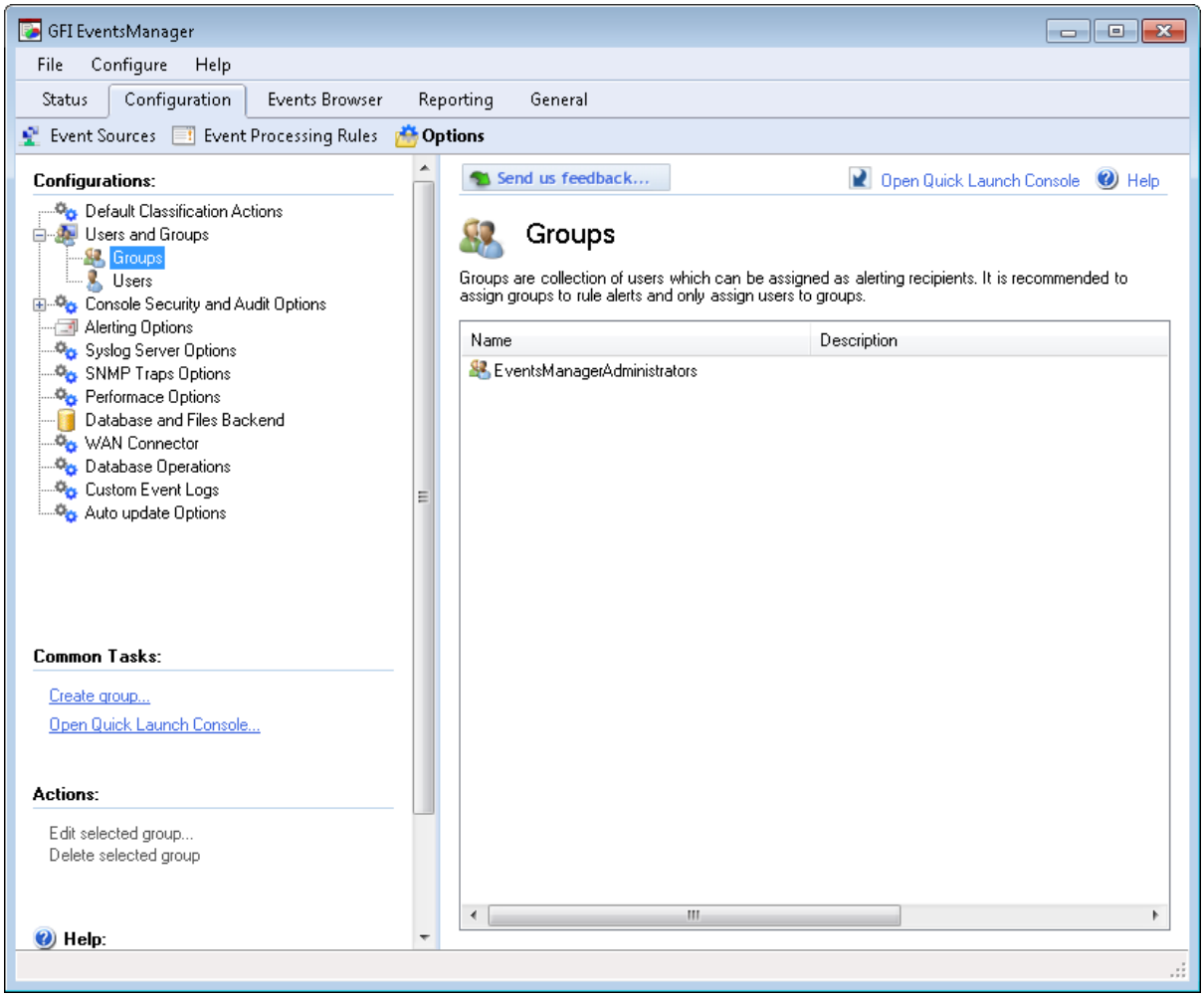
10.2.4 Deleting users

To delete a user:

1. From the left pane, click on the **Users** node.

2. From the right viewer pane, right-click on the user to be deleted and select **Delete**.

10.3 Manage groups



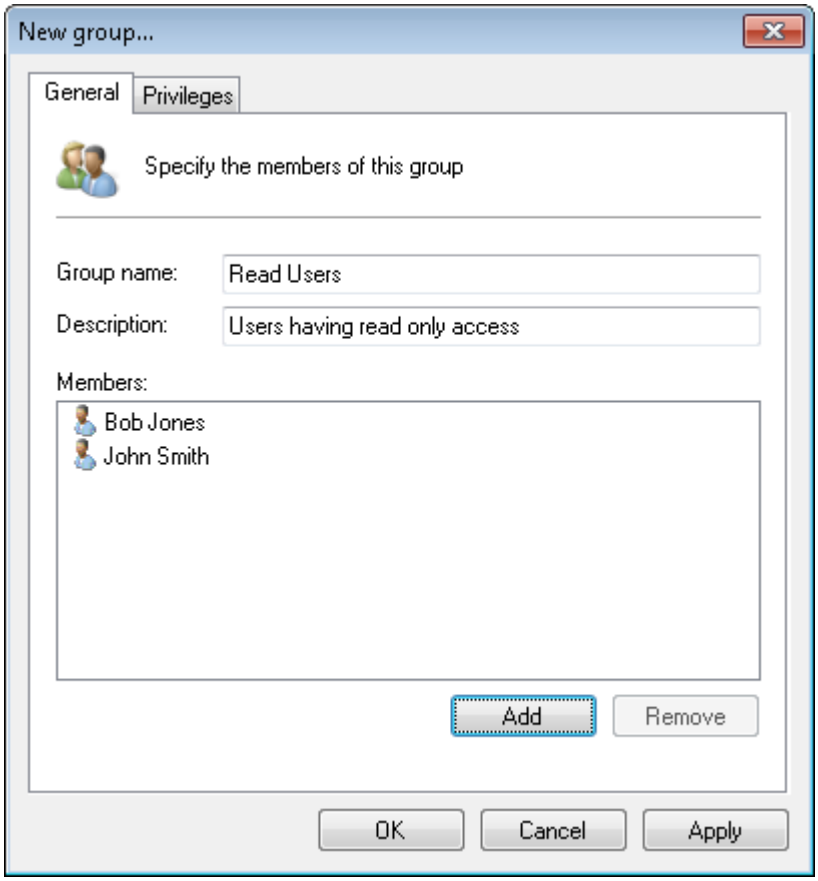
Screenshot 149 - Groups configuration screen

To create group:

1. Click **Configuration** tab and select **Options**.

2. Expand the **Users and Groups** node.

3. Right-click on the **Groups** sub-node and select **Create group…**



Screenshot 150 - New groups setup

4. Specify the name of the new group.

5. Click **Add** to start adding users to the group.

6. Click **OK** to finalize settings.

10.3.1 Changing user group properties

To edit the settings of a user group do as follows:

1. From the left pane, click on the **Groups** node.

2. From the right pane, right-click on the group to be configured and select **Properties**.

3. Perform the required changes in the tabs available and click **OK** to finalize settings.

10.3.2 Deleting user groups

To delete a user group:

1. From the left pane, click **Groups** node.

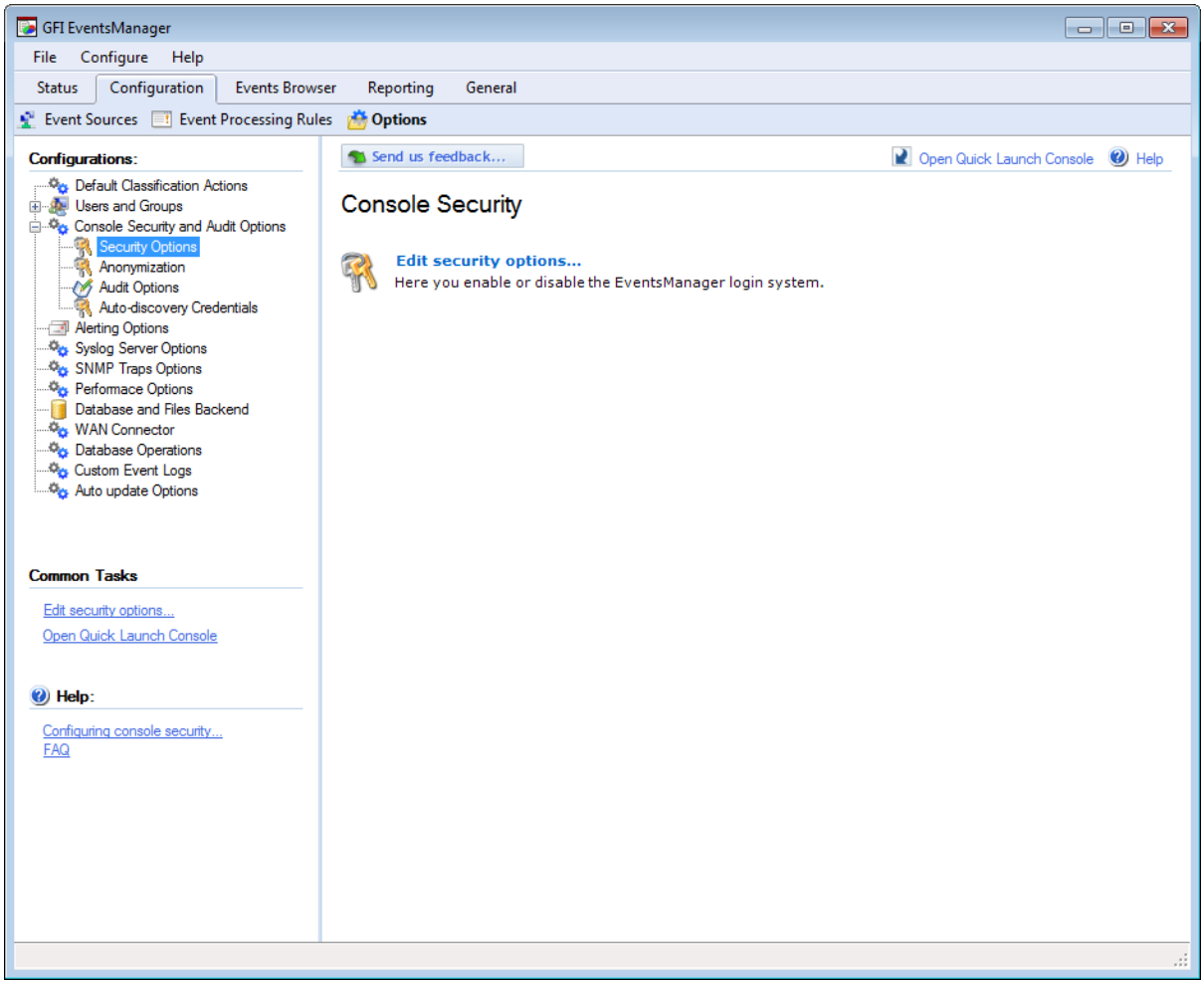
2. From the right viewer pane, right-click on the group to be deleted and select **Delete**.

10.4 Manage console security

10.4.1 GFI EventsManager login system

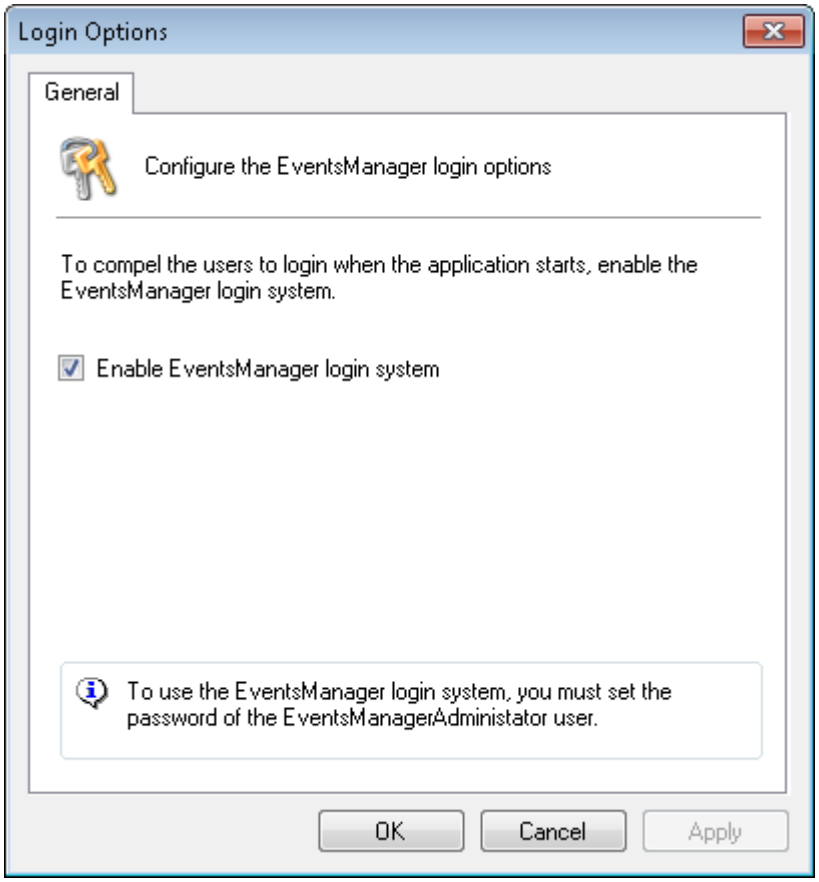
The Security Options node enables you to configure the GFI EventsManager login system.

1. Click **Configuration** tab and select **Options**.



Screenshot 151 - Select the login options feature

2. Expand **Console Security and Audit Options** node, click **Security Options** node and select **Edit security options…**.


Login Options
General
Configure the EventsManager login options
To compel the users to login when the application starts, enable the EventsManager login system.
Enable EventsManager login system
To use the EventsManager login system, you must set the password of the EventsManagerAdministator user.
OK
Cancel
Apply

Screenshot 152 - Login options dialog

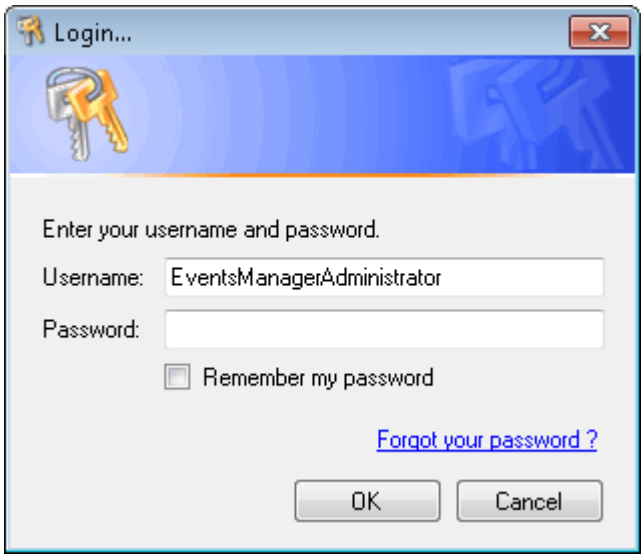
3. Select/unselect the Enable EventsManager login system option accordingly.

4. Click **OK** to finalize settings.

	When the login system is enabled all users will be asked to specify their credentials every time they launch the GFI EventsManager management console.
	Users are granted access with administrative or user privileges according to the user privileges set up in the privileges tab within the user setup dialogs.
	To configure or edit a user password, from **Configuration** tab ►**Users and Groups** ► **Users**, right-click the user account and select **Change Password**.

10.4.2 Password recovery

When GFI EventsManager login system is enabled, all users are requested to enter a valid user name and password to access GFI EventsManager console.



Screenshot 153 - Login window

If a password is forgotten or lost:

1. Key in your username.

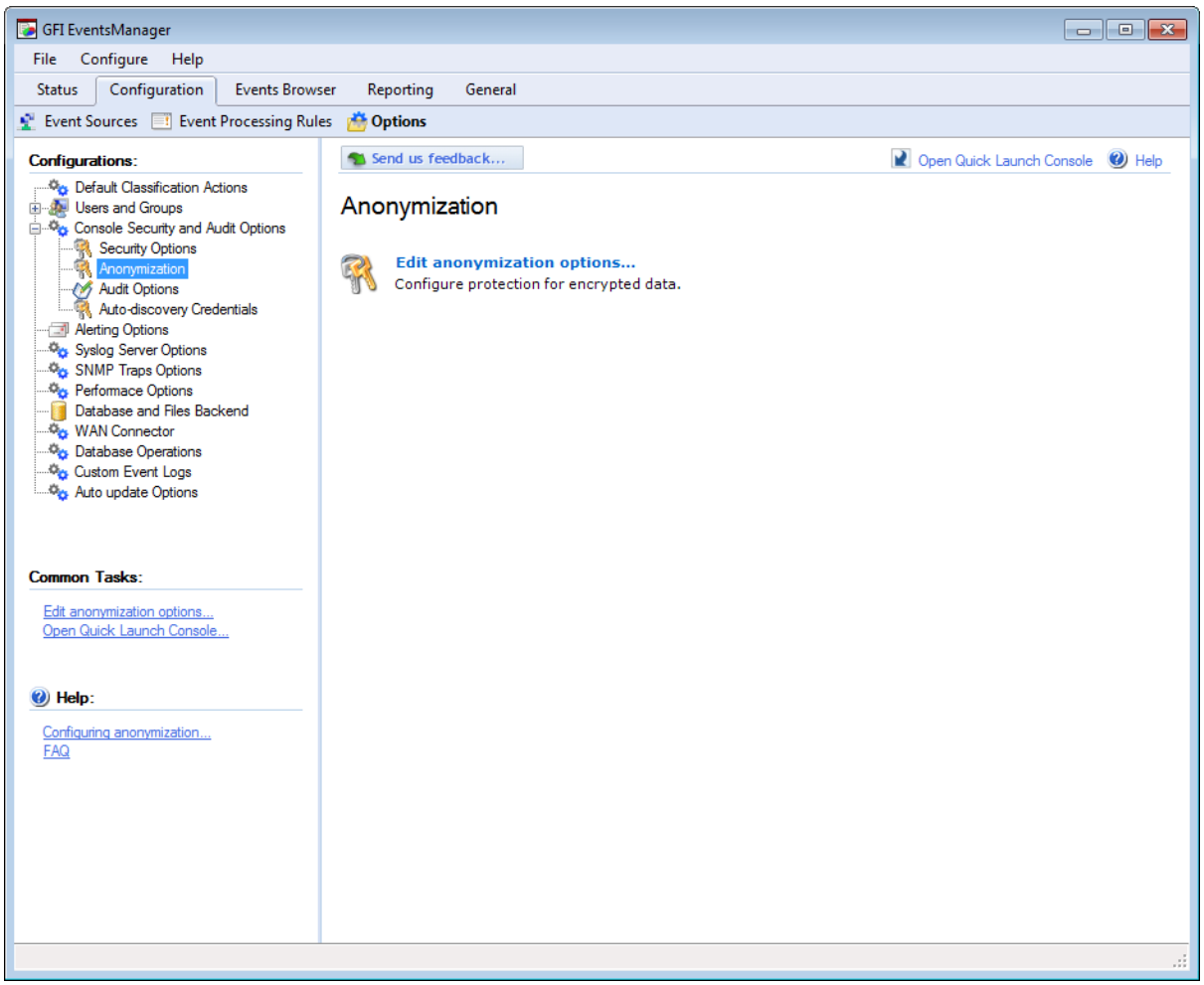
2. Click **Forgot your password?** Link

GFI EventsManager will send an email containing your login password.

	The User must have a valid email address configured in GFI EventsManager to receive the password by email. For more information on how to change user settings including the email address, refer to Changing user properties in this chapter.

10.4.3 Anonymization

In some countries privacy laws state that it is against the law not to encrypt personal information retrieved by monitoring applications for privacy protection.



Screenshot 154 - Anonymization

GFI EventsManager enables you to encrypt personal information when exporting and/or viewing event logs.

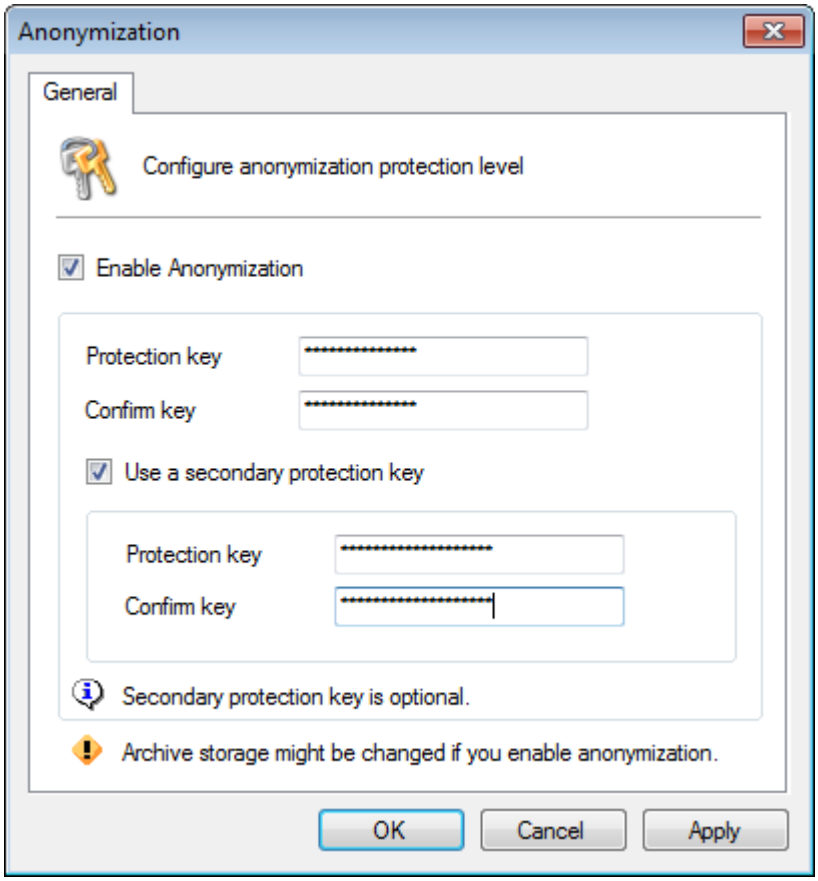
Enable anonymization to encrypt all personal information. The Events Browser and Dashboard can recognize such information and do not display it. Instead, they display **<encrypted>** or **Anonymized data** messages.

To configure anonymization:

1. From **Configuration** tab click **Options**.

2. Expand **Console Security and Audit Options** node, and click **Anonymization**.

3. Click **Edit anonymization options…**



Screenshot 155 - Anonymization options

4. Select **Enable Anonymization** and enter the encryption password.

5. (Optional) Select **Use a secondary protection key** to use two passwords for event log encryption. Event logs can only be decrypted by providing two decryption passwords.

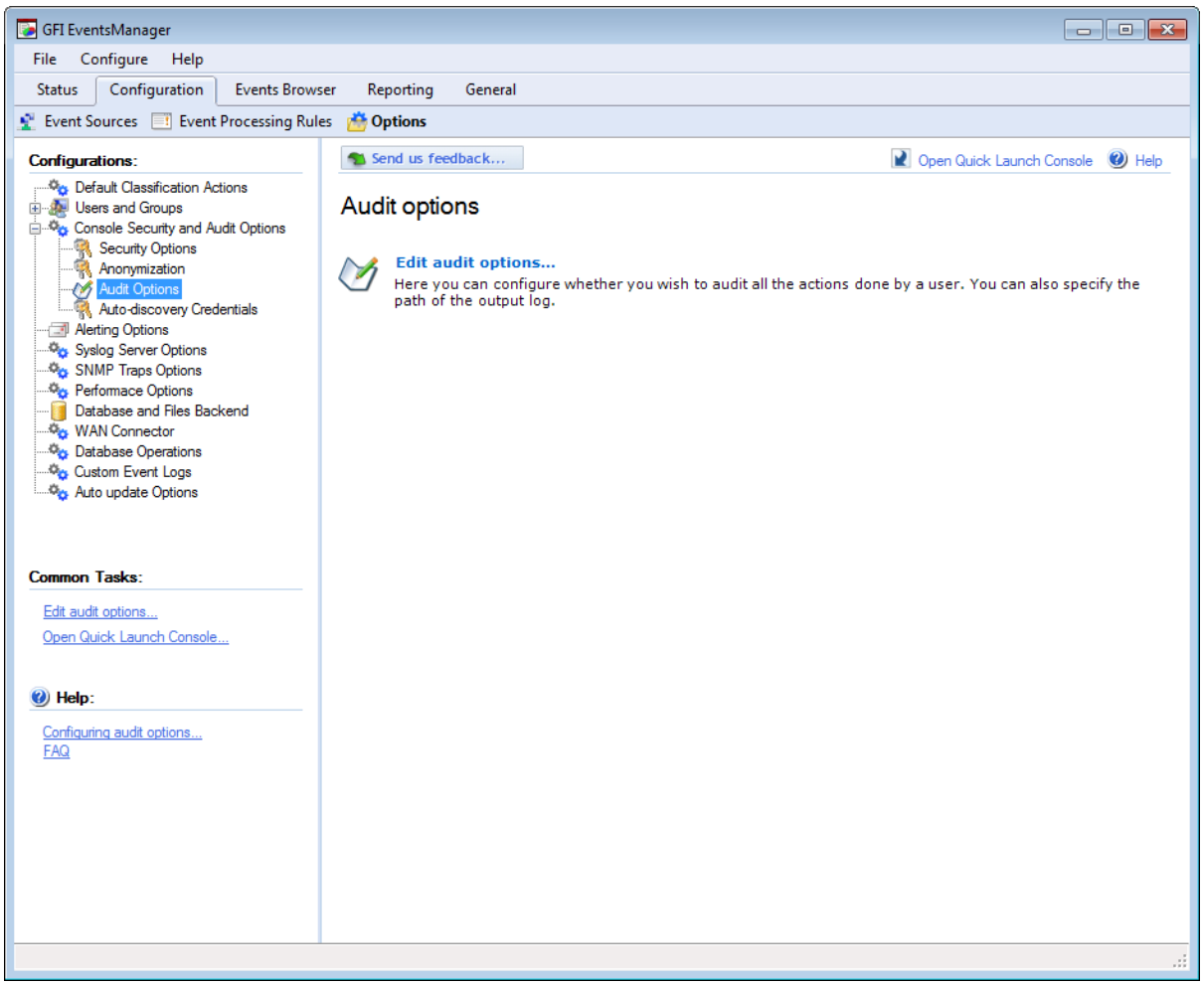
6. Click **OK** to finalize settings.

When anonymization is enabled, events that are stored into the central database are encrypted. For information on how to decrypt and/or re-encrypt databases, refer to Create new anonymization job section in this manual.

10.4.4 Audit console activity

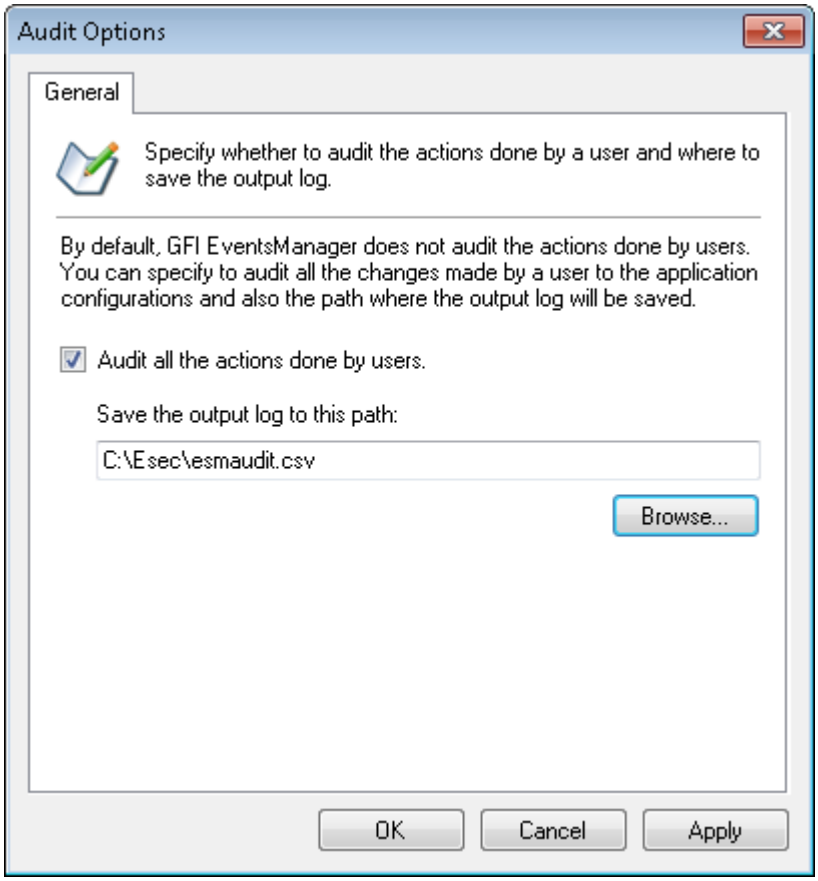
GFI EventsManager can save the console activity to external logs. To configure the console activity auditing:

1. Click **Configuration** tab and select **Options**.



Screenshot 156 - Select the Audit options feature

2. Expand **Console Security and Audit Options** node, click **Audit Options** node and select **Edit audit options…**.


Audit Options
General
Specify whether to audit the actions done by a user and where to save the output log.
By default, GFI EventsManager does not audit the actions done by users. You can specify to audit all the changes made by a user to the application configurations and also the path where the output log will be saved.
Audit all the actions done by users.
Save the output log to this path:
C:\Esec\esmaudit.csv
Browse...
OK
Cancel
Apply

Screenshot 157 - Audit Options

3. Select **Audit all the actions done by users** option and specify the location where the output log file will be saved.

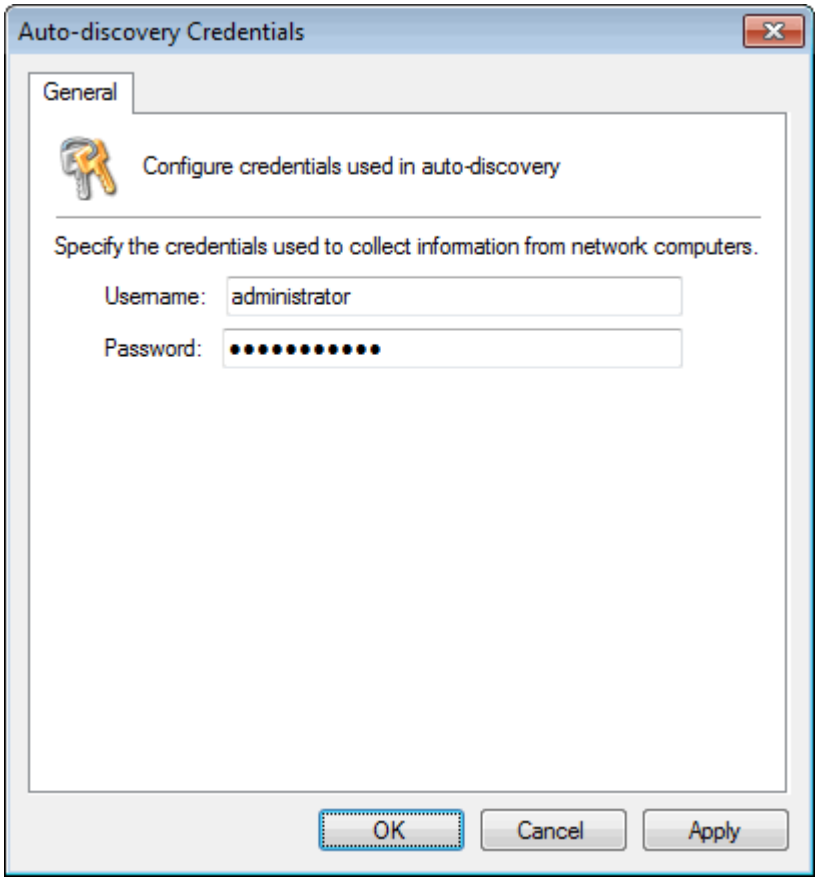
4. Click **OK** to finalize settings.

Reports related to the console activity can be generated using GFI ReportPack. For more information about GFI EventsManager ReportPack, refer to Generating reports chapter in this manual.

10.4.5 Auto-discovery credentials

The Auto-discovery credentials are used by GFI EventsManager to login target machines and collect information when performing an automatic search for event sources. To configure the auto-discovery credentials:

1. Click **Configuration ►Options** and under **Console Security and Audit Options**, select **Auto-discovery credentials ►Edit auto-discovery credentials**.



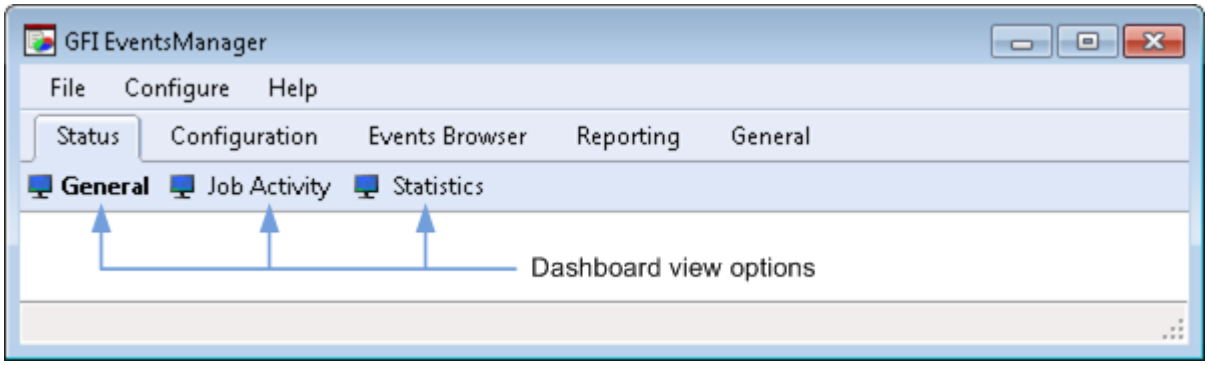
Screenshot 158 - Auto-discovery credentials

2. Key-in a valid username and password. Click **Ok**.

11 Status monitoring

11.1 Introduction

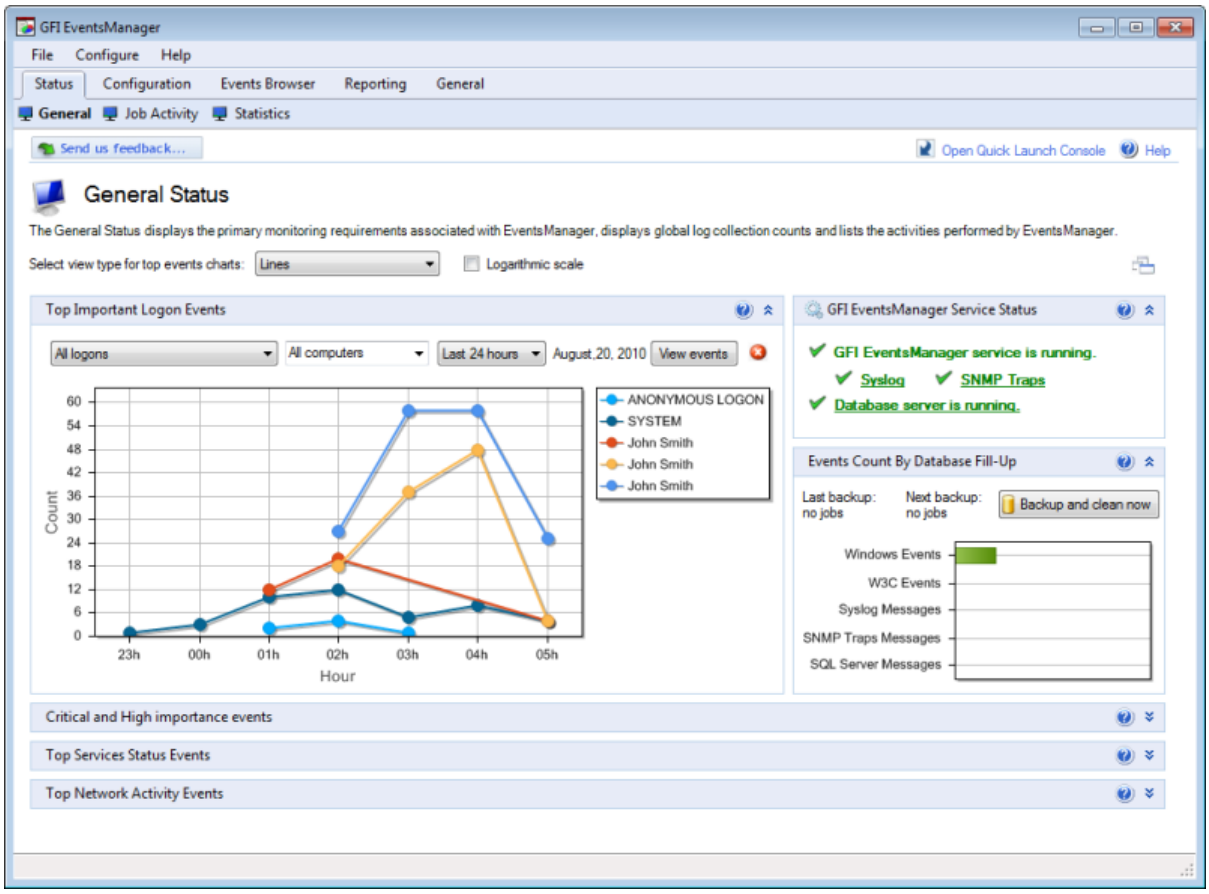
The status monitor is a dashboard that shows the status of GFI EventsManager as well as provides you with statistical information related to the events collected, processed and archived by this product. The status monitor consists of three different dashboard views: General view, Job Activity view and Statistics view.



Screenshot 159 - Dashboard View Options

To access the status monitor click on the **Status** tab and select the required dashboard view.

11.2 General status view



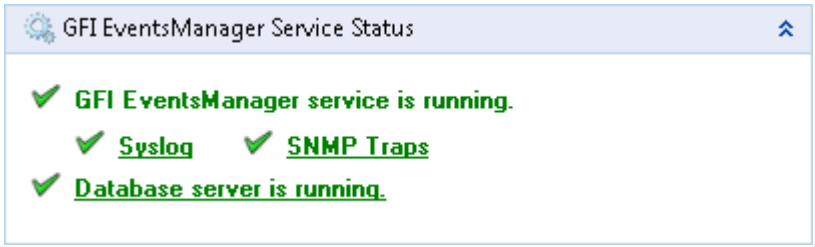
Screenshot 160 - GFI EventsManager status: General view

Use the **General** option to:

- View the status of the GFI EventsManager event processing engine.
- Access statistical information such as the number of logon events, critical events and service status events.

Click the **Arrange Window** icon to automatically fit all graphs in the management console.

11.2.1 GFI EventsManager service status



Screenshot 161 - GFI EventsManager General Status view: Service Status

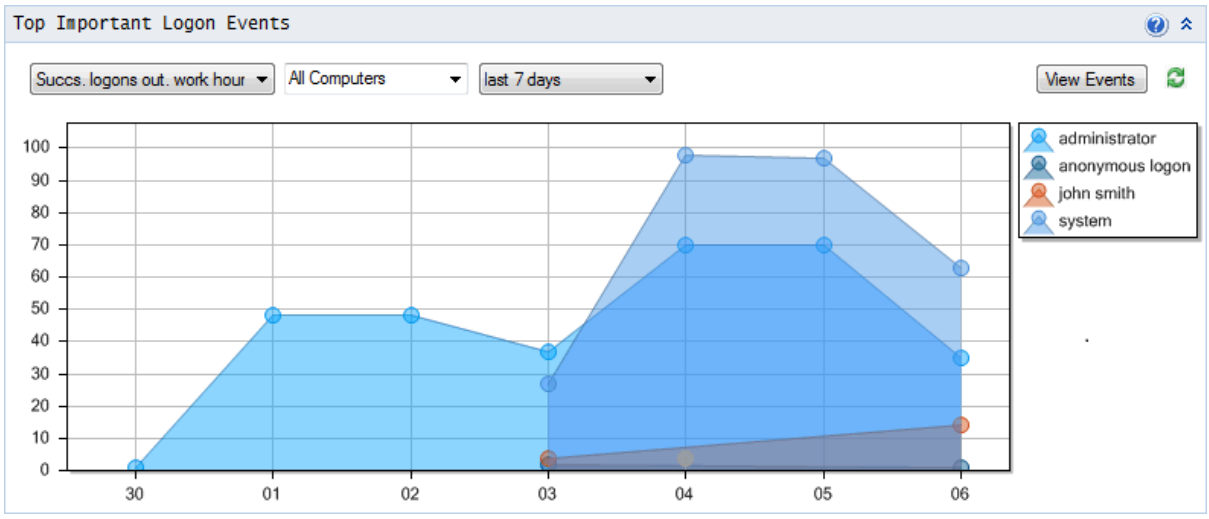
This section shows:

- The operational status of GFI EventsManager service/event processing engine
- The operational status of the Syslog server
- The operational status of the SNMP Traps server
- The operational status of the database server currently in use by GFI EventsManager

The GFI EventsManager service will not start if a database backend is not currently configured.

Click the service name to edit the service settings

11.2.2 Top Important Logon Events



Screenshot 162 - GFI EventsManager General Status view: Important logon events

This section provides statistical information about:

- Top 10 successful Logon events outside working hours
- Top 10 important Logon events during working hours
- Top 10 failed Logon events

Events in this section are filtered by:

- **Machine** - select a machine or key-in a machine name in the drop down list.
- **Period** - the time period when the events occurred (Last hour, Last 24 hours, Last 7 days or a specific date).

To view events in the **Events Browser**, click **View Events**. For more information on how to use the **Event Browser**, refer to Event browsing chapter in this manual.

Double click the graph to open the graph in a new window. When a 3D graph is selected, the new window allows you to rotate, zoom or resize the graph.

11.2.3 Critical and High Importance events

This section provides statistical/graphical information about critical events collected from all event sources. This graph shows the event processing rules that collected and processed the events for a particular period. For detailed information about the different types of important events shown in this graph, download the **Microsoft Security Monitoring and Attack Detection Planning Guide** from http://www.gfi.com/ms-security-mointoring-and-attack-detection-planning/.

Screenshot 163 - GFI EventsManager General Status view: Critical and High importance events

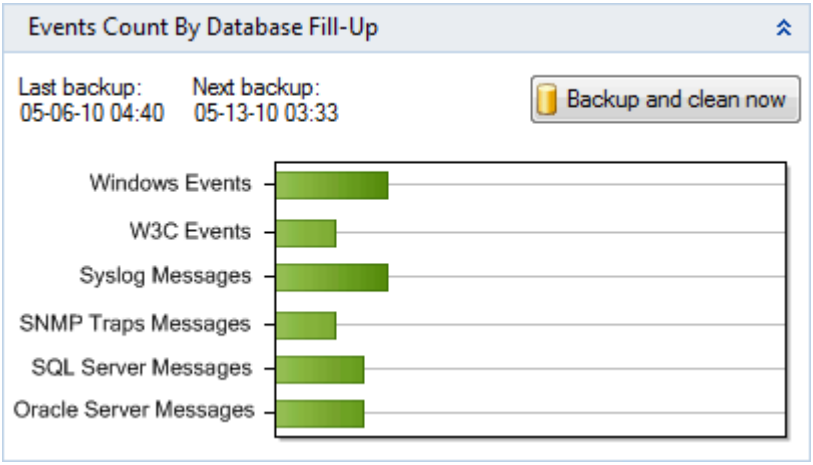
From the drop down lists, select the type of information to display:

- **Grouping** - how events are grouped (by Events, Computers, Computer groups, Events/Computers or Events/Computer groups)
- **Event type** - the type of data to display (Windows, W3C, Syslog, SNMP, SQL and Oracle audit).
- **Alert type** - the alert type (All alerts, Critical or High)
- **Period** - the time period when the events occurred (Last hour, Last 24 hours, Last 7 days or a specific date).

To view events in the **Events Browser**, click **View Events**. For more information on how to use the **Event Browser**, refer to Event browsing chapter in this manual.

	Double click the graph to open the graph in a new window. When a 3D graph is selected, the new window allows you to rotate, zoom or resize the graph.
	The **Top Critical and High Importance Events** also display the vulnerability results monitored by GFI LANguard. For more information, refer to Adding GFI LANguard event sources section in this manual.

11.2.4 Events Count by Database Fill-Up



Screenshot 164 - GFI EventsManager General Status view: Service Status

This section displays:

- The horizontal bars represent the number of events stored in the database backend, sorted by event log type.
- The date and time of the last backup
- The date and time of the next scheduled backup.

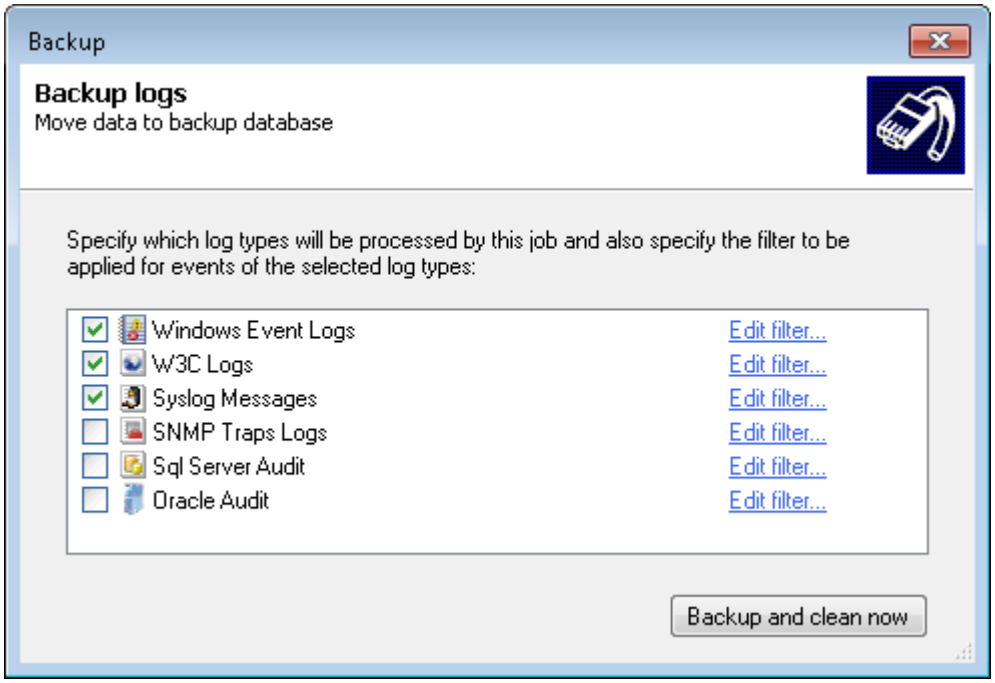
The bar color turns from green to red as the database is populated with events. It is recommended to perform a backup when the horizontal bar reaches the full (red) status. For more information on how to create a new database backup and maintenance jobs, refer to Create maintenance jobs section in this manual.

Backup and Clean now

To start a backup operation:

1. Click **Backup and Clean now**.

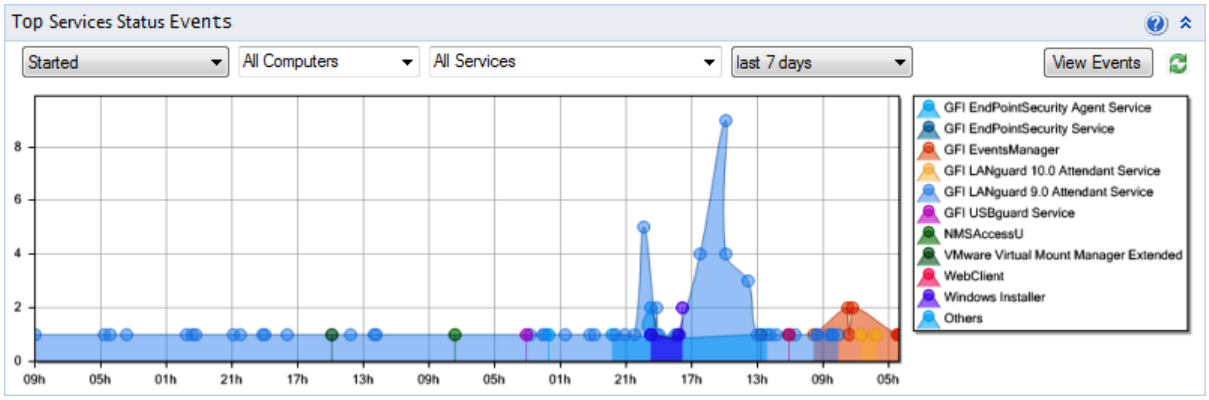
2. Select which events for backup and click **Backup and clean now**.


Backup
Backup logs
Move data to backup database
Specify which log types will be processed by this job and also specify the filter to be applied for events of the selected log types:
Windows Event Logs
W3C Logs
Syslog Messages
SNMP Traps Logs
Sql Server Audit
Oracle Audit
Edit filter...
Backup and clean now

Screenshot 165 - GFI EventsManager Backup logs

If the **Backup and Clean now** is disabled, create a new database operation job. For more information on how to create a new database operation, refer to Create maintenance jobs section in this manual.

11.2.5 Top Services Status Events



Screenshot 166 - GFI EventsManager General Status view: Services Status

This section displays the top 10 services that caused the selected event. A service can generate events when:

- Terminated with an error
- Failed to load
- Failed to start
- Timed out
- Stopped
- Started

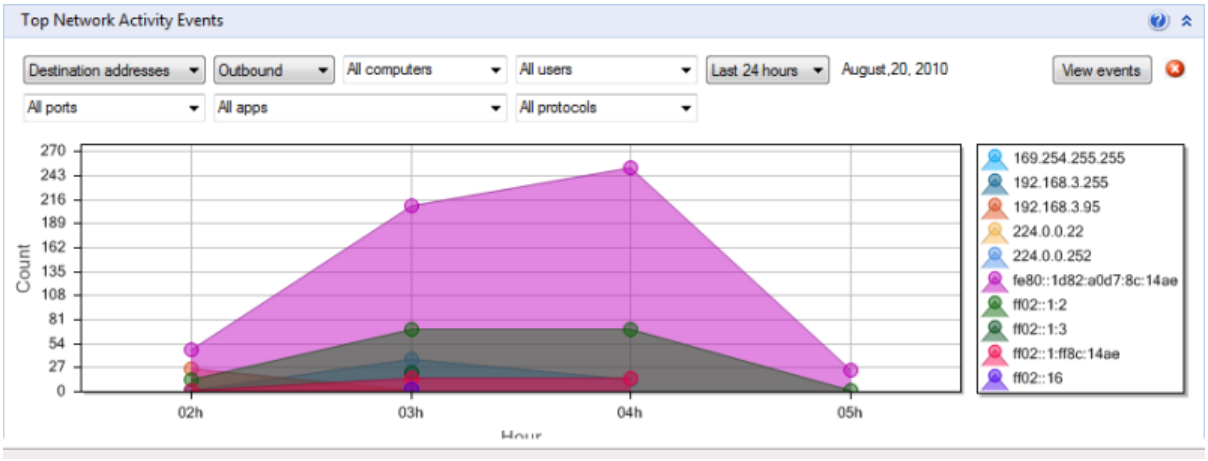
The graph shows the frequency of these events sorted by service type or\and by computer generating the event. Select a machine or service from the drop down lists or key-in the required criteria to customize the graph results.

To view events in the **Events Browser**, click **View Events**. For more information on how to use the **Event Browser**, refer to Event browsing chapter in this manual.

To collect services information, target machines must have Audit system events policy enabled. For more information on how to enable this audit policy, refer to Step 2: Enable additional auditing features section in this manual.

Double click the graph to open the graph in a new window. When a 3D graph is selected, the new window allows you to rotate, zoom or resize the graph.

11.2.6 Top Network Activity Events



Screenshot 167 - GFI EventsManager General Status view: Network Activity

This section displays details of the top 10 network activities (inbound and outbound) generated by target machines. Network activity consists of all type of traffic that is generated by various protocols including SMTP, HTTP, FTP and MSN traffic. The network activities displayed can be filtered by:

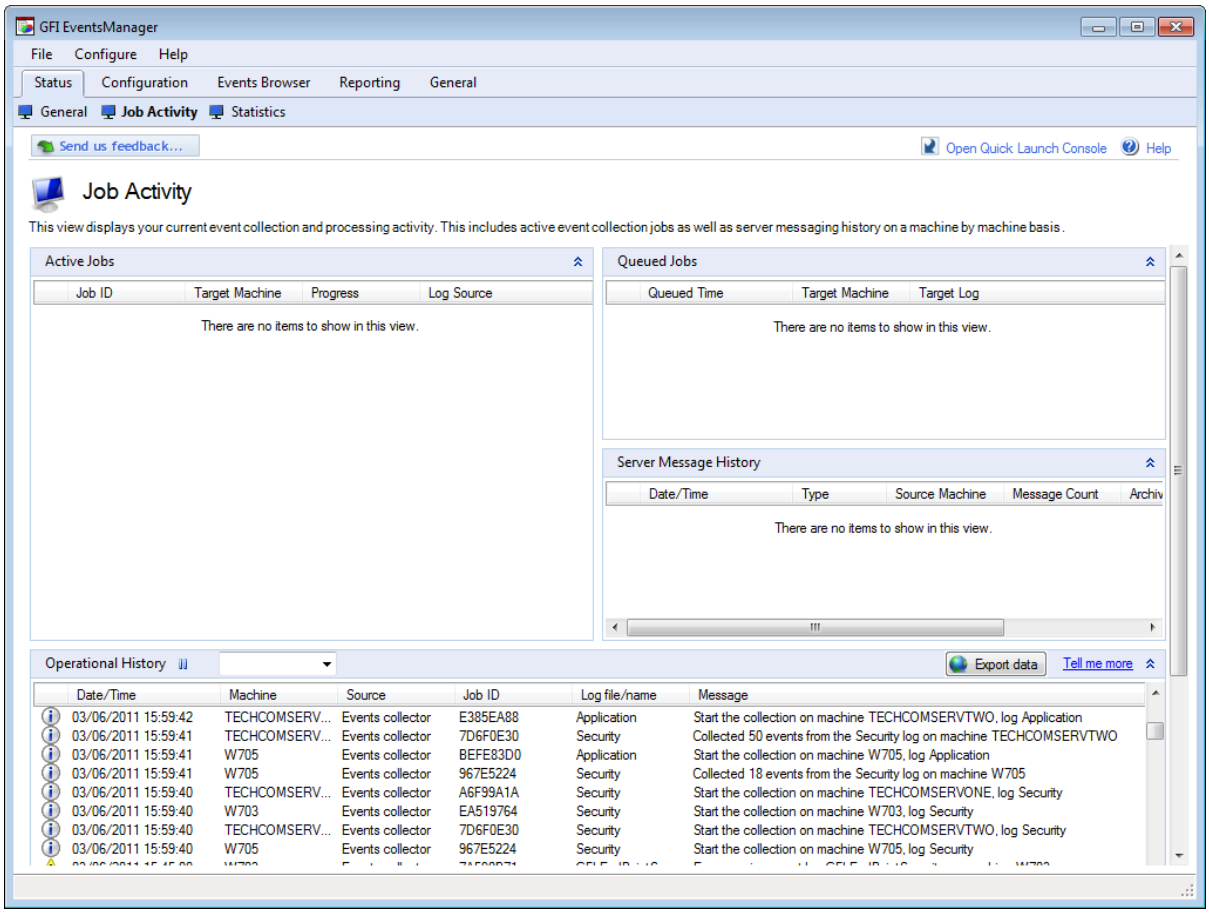
- Applications
- Source Addresses
- Destination Addresses
- Computers
- Ports
- Users

Select parameters from the drop down lists or key-in the values to filter the type of chart displayed.

The network activity shown in the chart applies only to computers running Microsoft Windows Vista or later.

To collect network activities, target machines must have **Object auditing** and **Process tracking** enabled. For more information on how to enable these audit policies, refer to Step 2: Enable additional auditing features section in this manual.

11.3 Job activity view

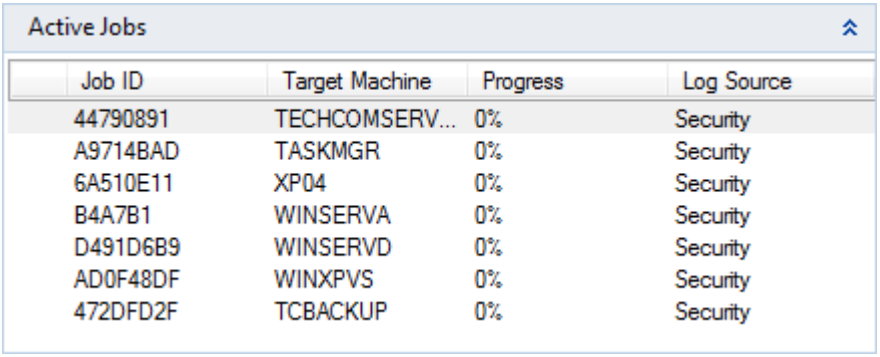

GFI EventsManager
File Configure Help
Status Configuration Events Browser Reporting General
General Job Activity Statistics
Send us feedback...
Open Quick Launch Console Help
Job Activity
This view displays your current event collection and processing activity. This includes active event collection jobs as well as server messaging history on a machine by machine basis.
Active Jobs
Job ID Target Machine Progress Log Source
There are no items to show in this view.
Queued Jobs
Queued Time Target Machine Target Log
There are no items to show in this view.
Server Message History
Date/Time Type Source Machine Message Count
There are no items to show in this view.
Operational History
Export data Tell me more
Date/Time Machine Source Job ID Log file/name Message
03/06/2011 15:59:42 TECHCOMSERV... Events collector E385EA88 Application Start the collection on machine TECHCOMSERVTWO, log Application
03/06/2011 15:59:41 TECHCOMSERV... Events collector 7D6F0E30 Security Collected 50 events from the Security log on machine TECHCOMSERVTWO
03/06/2011 15:59:41 W705 Events collector BEFE83D0 Application Start the collection on machine W705, log Application
03/06/2011 15:59:41 W705 Events collector 967E5224 Security Collected 18 events from the Security log on machine W705
03/06/2011 15:59:40 TECHCOMSERV... Events collector A6F99A1A Security Start the collection on machine TECHCOMSERVONE, log Security
03/06/2011 15:59:40 W703 Events collector EA519764 Security Start the collection on machine W703, log Security
03/06/2011 15:59:40 TECHCOMSERV... Events collector 7D6F0E30 Security Start the collection on machine TECHCOMSERVTWO, log Security
03/06/2011 15:59:40 W705 Events collector 967E5224 Security Start the collection on machine W705, log Security

Screenshot 168 - GFI EventsManager Job Activity view

This view displays your current event collection and processing activity. This includes active event collection jobs as well as server messaging history on a machine by machine basis.

The information provided in this view is divided into dedicated sections. More details on these sections are provided below.

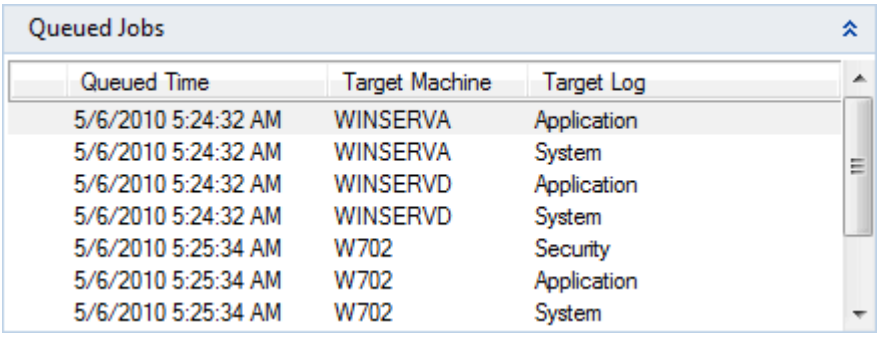
11.3.1 Active jobs


Active Jobs
Job ID Target Machine Progress Log Source
44790891 TECHCOMSERV... 0% Security
A9714BAD TASKMGR 0% Security
6A510E11 XP04 0% Security
B4A7B1 WINSERVA 0% Security
D491D6B9 WINSERVD 0% Security
AD0F48DF WINXPVS 0% Security
472DFD2F TCBACKUP 0% Security

Screenshot 169 - GFI EventsManager Job Activity view: Active Jobs

This section shows a list of all event collection jobs currently taking place on every event source/machine. The information provided includes the job progress as well as the Log Source from which events are being collected.

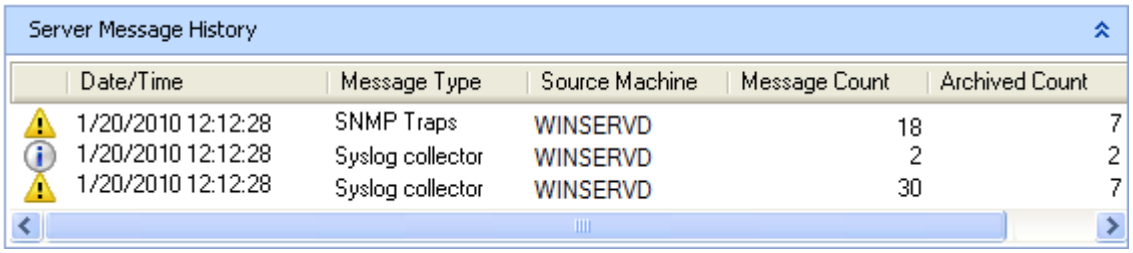
11.3.2 Queued jobs



Screenshot 170 - GFI EventsManager Job Activity view: Queued Jobs

This section shows a list of all pending event collection jobs on a machine by machine basis. The information provided includes the Log Source from which events will be collected as well as the time that these jobs were queued.

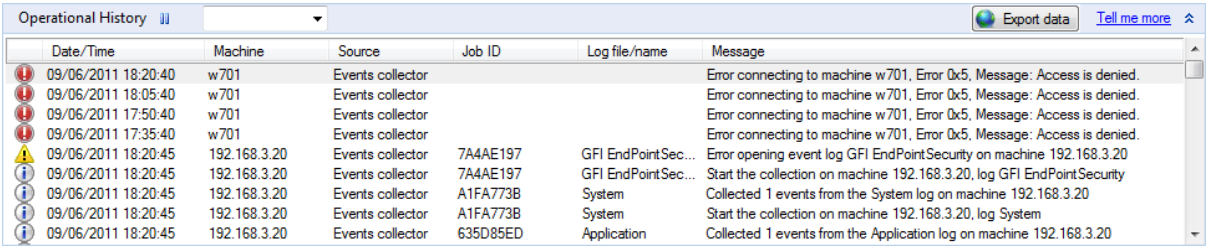
11.3.3 Server message history



Screenshot 171 - GFI EventsManager Job Activity view: Server Message History

This section shows a list of all server messages (SNMP Traps and Syslog) that were received by GFI EventsManager. The information provided includes the total number of messages sent by every source machine and the date/time when the last message was received.

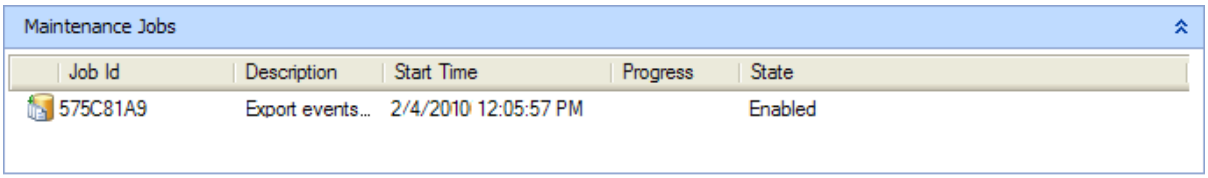
11.3.4 Operational history


Operational History
Export data
Tell me more
Date/Time Machine Source Job ID Log file/name Message
09/06/2011 18:20:40 w701 Events collector Error connecting to machine w701, Error 0x5, Message: Access is denied.
09/06/2011 18:05:40 w701 Events collector Error connecting to machine w701, Error 0x5, Message: Access is denied.
09/06/2011 17:50:40 w701 Events collector Error connecting to machine w701, Error 0x5, Message: Access is denied.
09/06/2011 17:35:40 w701 Events collector Error connecting to machine w701, Error 0x5, Message: Access is denied.
09/06/2011 18:20:45 192.168.3.20 Events collector 7A4AE197 GFI EndPointSec... Error opening event log GFI EndPointSecurity on machine 192.168.3.20
09/06/2011 18:20:45 192.168.3.20 Events collector 7A4AE197 GFI EndPointSec... Start the collection on machine 192.168.3.20, log GFI EndPointSecurity
09/06/2011 18:20:45 192.168.3.20 Events collector A1FA773B System Collected 1 events from the System log on machine 192.168.3.20
09/06/2011 18:20:45 192.168.3.20 Events collector A1FA773B System Start the collection on machine 192.168.3.20, log System
09/06/2011 18:20:45 192.168.3.20 Events collector 635D85ED Application Collected 1 events from the Application log on machine 192.168.3.20

Screenshot 172 - GFI EventsManager Job Activity view: Operational History

This section shows an audit trail of the event collection operations carried out by GFI EventsManager. The information provided includes errors and information messages generated during the event collection process as well as the name of the log file that was being processed on the source machine.

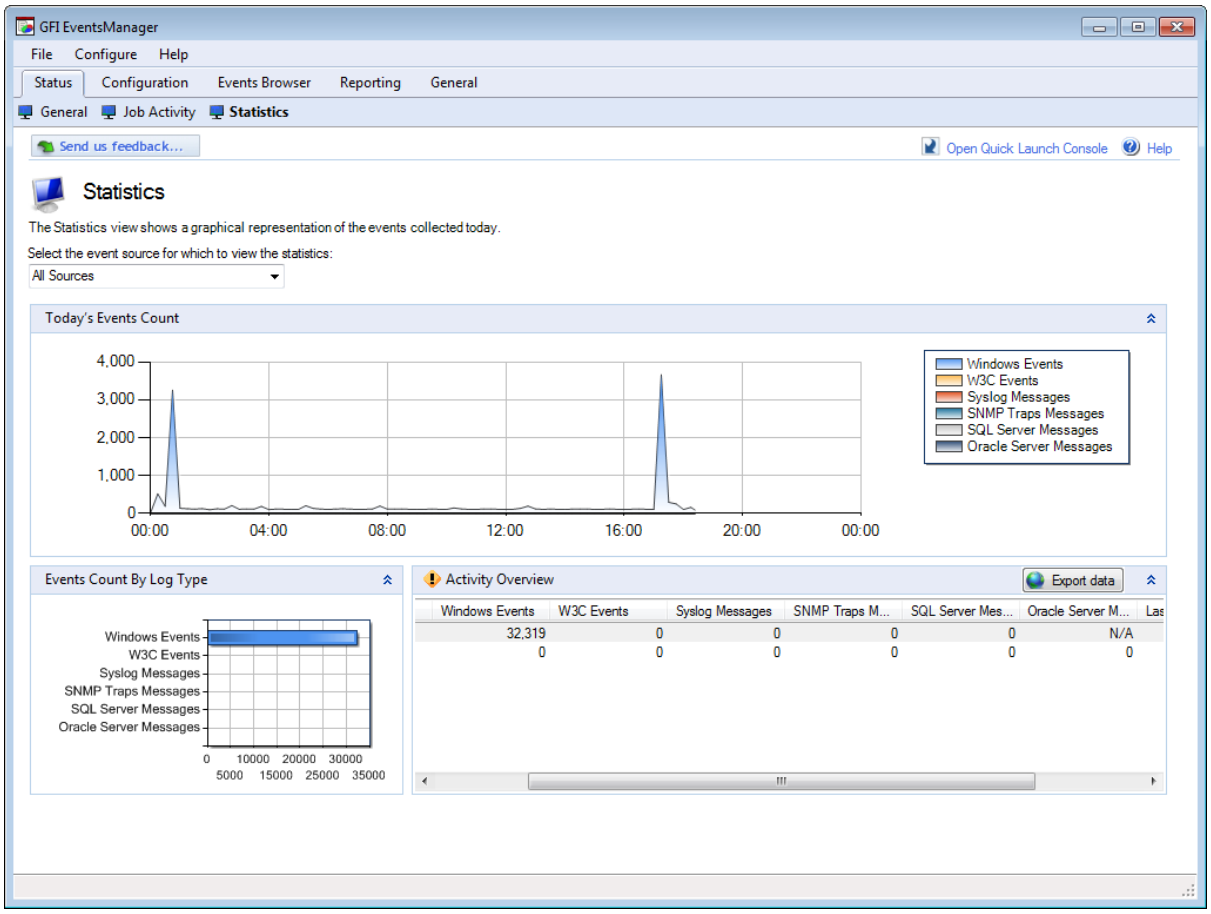
11.3.5 Maintenance jobs



Screenshot 173 - GFI EventsManager Job Activity view: Job activity status

This section shows the progress of maintenance jobs that have been created through **Database Operations**. The information provided includes the job description as well as the time when the job began execution.

11.4 Statistics view

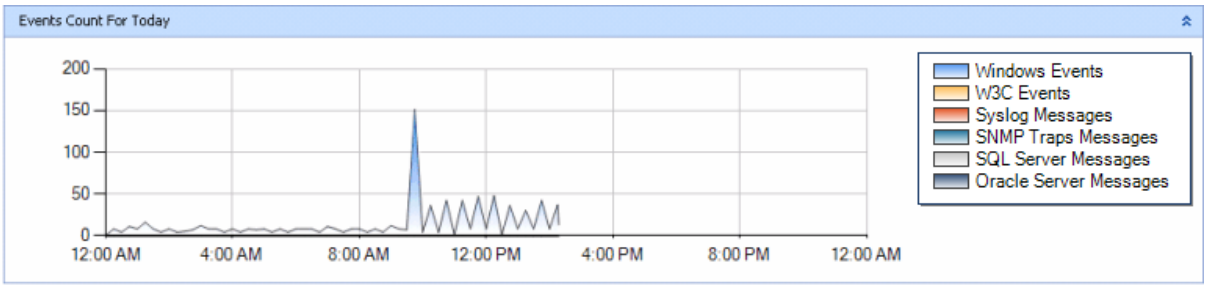


Screenshot 174 - GFI EventsManager Statistics view

Use the **Statistics** option to view the daily event activity trends and statistics of a particular computer or of your entire network.

The information provided in this view is divided into dedicated sections. More details on these sections are provided below.

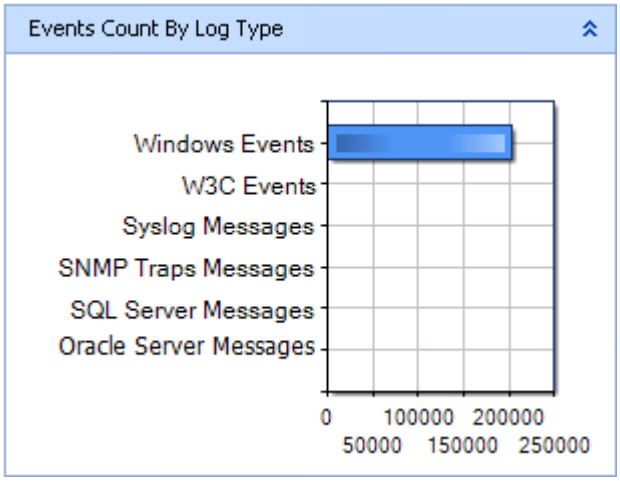
11.4.1 Events count for today



Screenshot 175 - GFI EventsManager Statistics view: Events Count For Today

This section graphically represents the daily event collection trend on a machine by machine basis as well as on a network by network basis. A color scheme is used to differentiate between Windows, W3C, Syslog and SNMP Traps events.

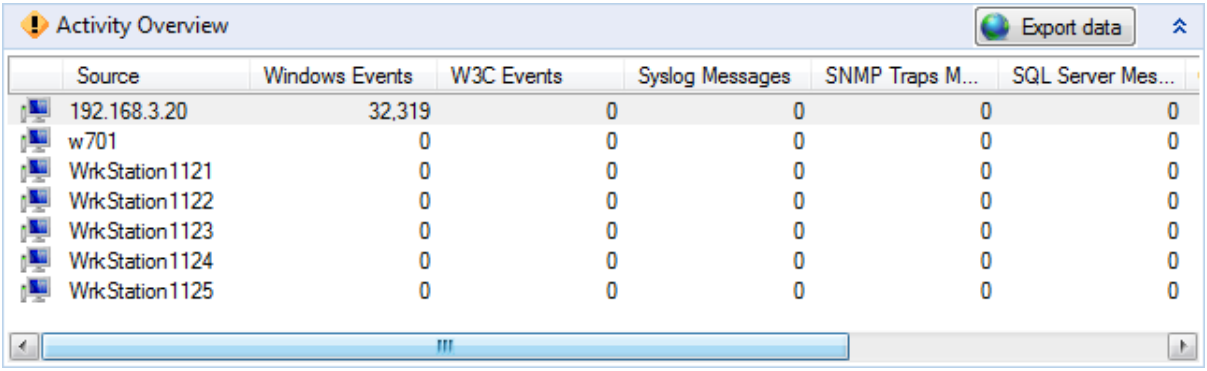
11.4.2 Events count by log type



Screenshot 176 - GFI EventsManager Statistics view: Events count by log type

This section graphically represents the number of Windows, W3C, Syslog and SNMP Traps events collected by GFI Events Manager from a particular machine or network.

11.4.3 Activity overview



Source	Windows Events	W3C Events	Syslog Messages	SNMP Traps M...	SQL Server Mes...
192.168.3.20	32,319	0	0	0	0
w701	0	0	0	0	0
WrkStation1121	0	0	0	0	0
WrkStation1122	0	0	0	0	0
WrkStation1123	0	0	0	0	0
WrkStation1124	0	0	0	0	0
WrkStation1125	0	0	0	0	0

Screenshot 177 - GFI EventsManager Statistics view: Activity Overview

This section shows:

- The total number of Windows, W3C, Syslog and SNMP Traps events processed on a machine by machine basis
- The date/time of the last event collection performed from every machine.

12 Database Operations

12.1 Introduction

The Database Operations module in GFI EventsManager provides advanced functionality allowing administrators to:

- Centralize events collected by other remote GFI EventsManager instances into one database backend.
- Optimize GFI EventsManager performance by actively controlling database backend growth hence keeping it in good shape.
- Import and export data to and from GFI EventsManager version 8.x installations without data inconsistencies.
- Import and export events to and from a storage folder minimizing data loads from the database.

12.2 Why database maintenance?

Periodical database maintenance is essential in preventing excessive data growth in the database backend. A database which is large in size drastically affects the performance of GFI EventsManager; events browsing will be slower and queries will take longer to execute. There will also be a negative impact on GFI EventsManager ReportPack performance, with reports taking longer to be generated.

Through GFI EventsManager a number of database operations, referred to as maintenance jobs, can be carried out on the database backend. These include:

- **Move to database** - Use this operation to move events from the main database to the backup database or to another existing database.
- **Export to file** - Use this operation to export events from the main database to a compressed binary file which can also be encrypted and backed to CD/DVD or tape for safekeeping.
- **Import from file** - Use this operation to import events from GFI EventsManager export files into the main database backend.
- **Delete data** - Use this operation to remove events from the main or backup database back-ends.

Filters that determine which events will be affected by the database operation can be applied for each operation.

Consolidation of events for a WAN

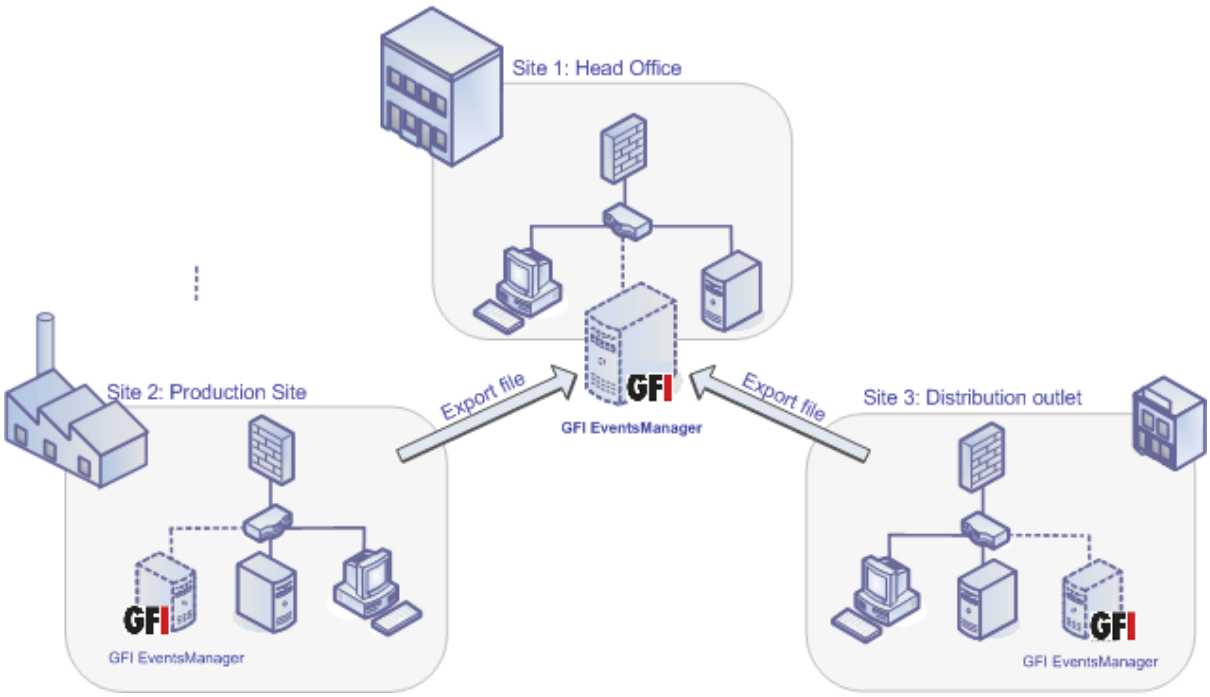


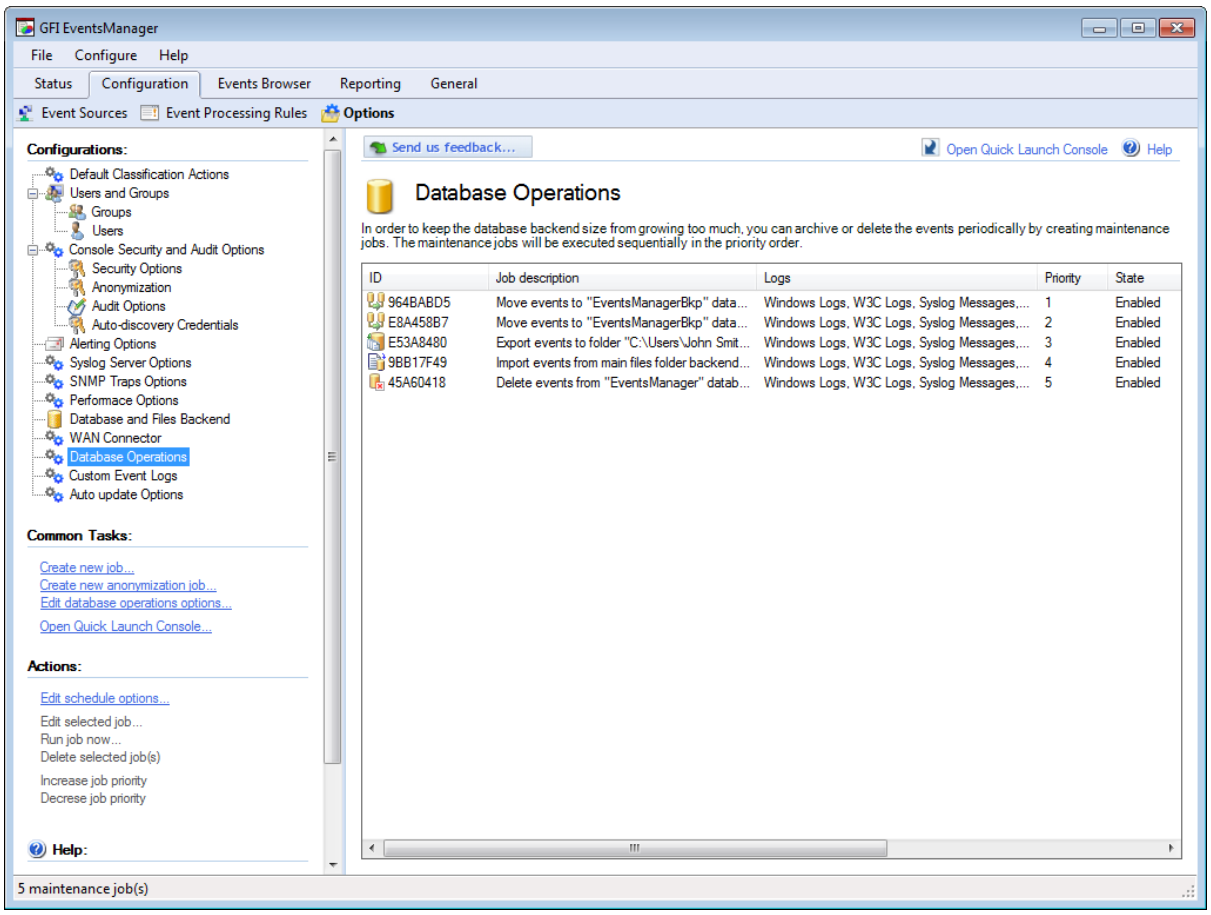
Figure 9: Consolidation of events for a WAN

In the case of organizations with remote geographical sites, Database Operations can be used to consolidate all or part of the events data collected in remote sites on to one central database. This is achieved using the 'Export to file' feature through which GFI EventsManager compresses and encrypts the file as well as export the file to be processed to a central location. The 'Import to file' job is executed at the central location, importing the events from the remote site into the central database.

Events for the remote site can then be viewed through the Events Browser. Reports with information relevant to the remote site can also be generated using data from the central database.

12.3 Create maintenance jobs

With GFI EventsManager you can schedule maintenance jobs to be executed on a specific day, at a specific time and at specific intervals.



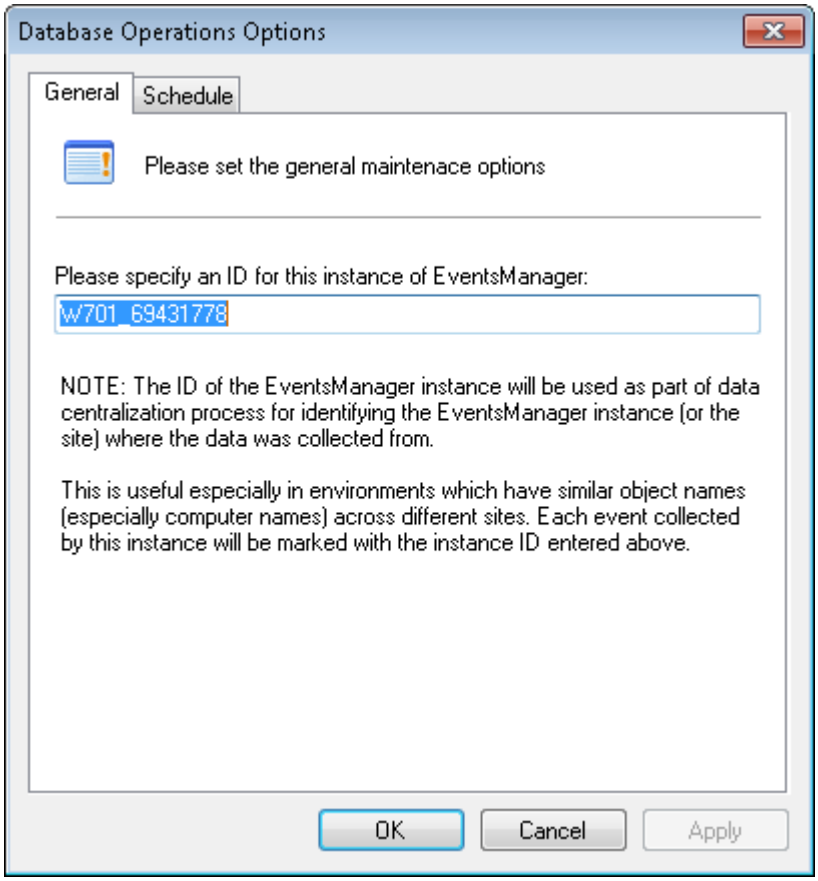
Screenshot 178 - Configuring Database Operations

Database maintenance operations may require high utilization of resources which can degrade server and GFI EventsManager performance. Thus, it is recommended that you schedule maintenance jobs to be executed after office hours. This allows you to maximize the availability of your system resources during working hours and avoid any possible disruptions to workflow.

To configure Database Operations:

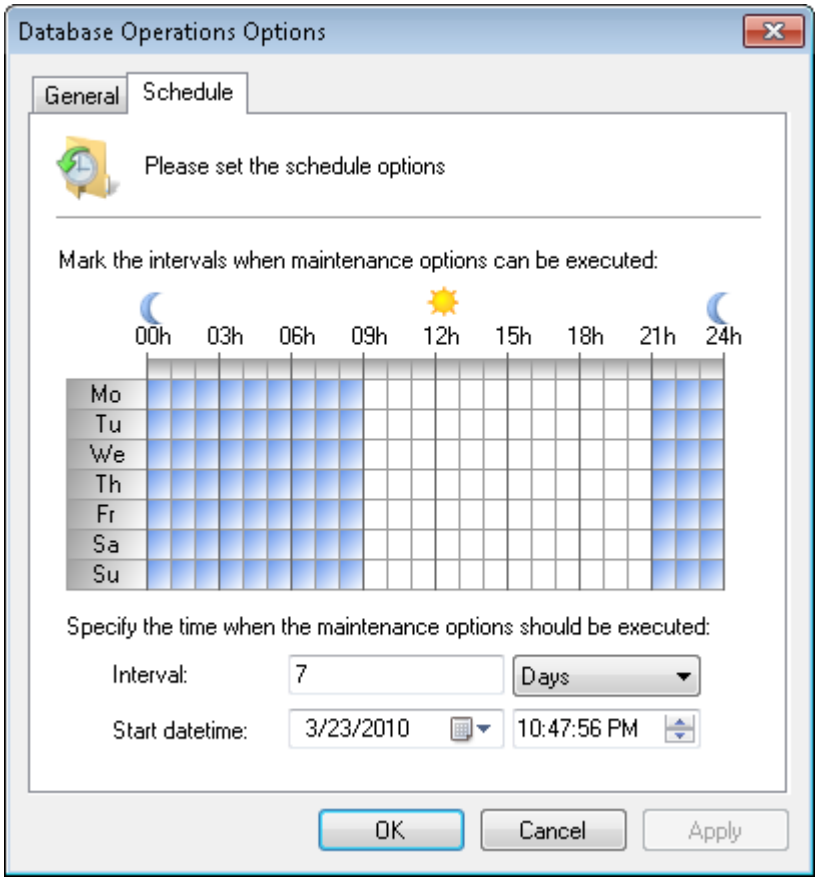
1. Click **Configuration** tab and select **Options**.

2. From the left pane, right-click on the **Database Operations** node and select **Properties**.


Database Operations Options
General
Schedule
Please set the general maintenace options
Please specify an ID for this instance of EventsManager:
W701_69431778
NOTE: The ID of the EventsManager instance will be used as part of data centralization process for identifying the EventsManager instance (or the site) where the data was collected from.
This is useful especially in environments which have similar object names (especially computer names) across different sites. Each event collected by this instance will be marked with the instance ID entered above.
OK
Cancel
Apply

Screenshot 179 - Database Operations Options dialog: GFI EventsManager unique identifier

3. Specify the unique identifier by which this instance of GFI EventsManager will be identified on the network. This identifier is used as part of the export file-name during 'Export to file' operations.



Screenshot 180 - Database Operations Options dialog: Scheduling options

4. Click **Schedule** tab to specify:

» Hours of the day during which maintenance jobs can be executed

» The interval in hours/days with which maintenance jobs will be executed

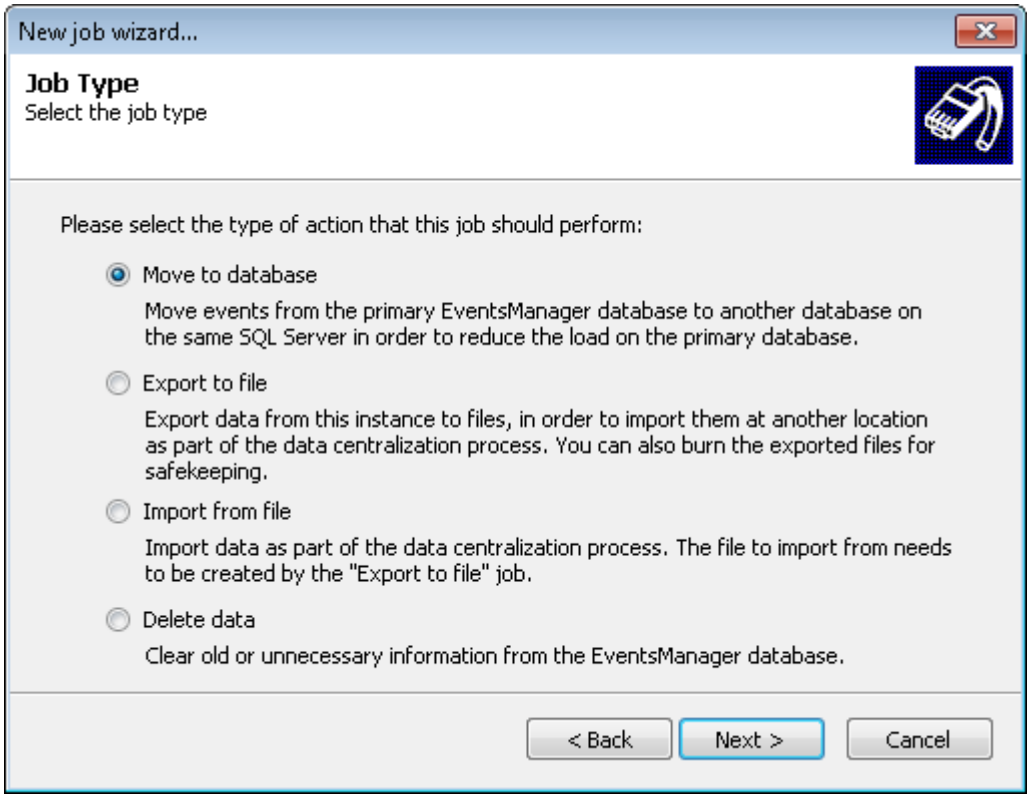
» The scheduled date/time when maintenance jobs will start being executed.

To create a new maintenance job:

1. Click **Configuration** tab and select **Options**.

2. From the left pane, right-click **Database Operations** node and select **Create new job…**

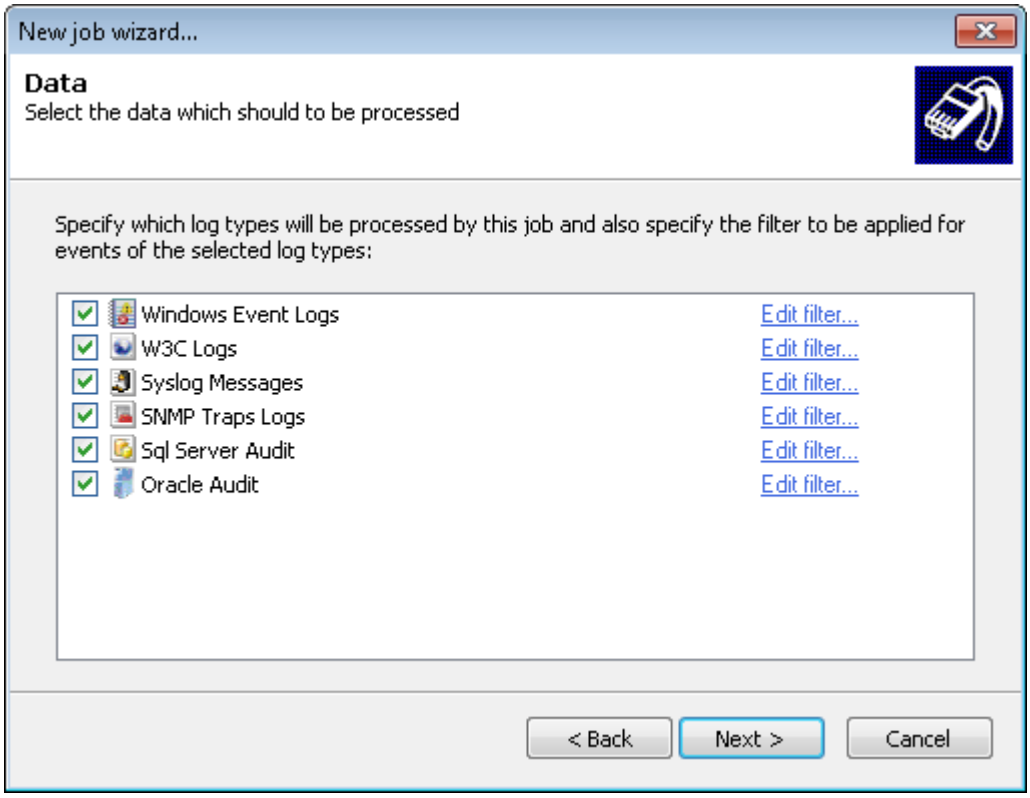
3. Click **Next** button.


New job wizard...
Job Type
Select the job type
Please select the type of action that this job should perform:
Move to database
Move events from the primary EventsManager database to another database on the same SQL Server in order to reduce the load on the primary database.
Export to file
Export data from this instance to files, in order to import them at another location as part of the data centralization process. You can also burn the exported files for safekeeping.
Import from file
Import data as part of the data centralization process. The file to import from needs to be created by the "Export to file" job.
Delete data
Clear old or unnecessary information from the EventsManager database.
< Back
Next >
Cancel

Screenshot 181 - New job wizard: Job Type dialog

4. Select the type of maintenance job you want to create and click **Next** to proceed to the configuration dialog.

5. Specify the required parameters and click **Next** to proceed to the data filter configuration dialog.


New job wizard...
Data
Select the data which should to be processed
Specify which log types will be processed by this job and also specify the filter to be applied for events of the selected log types:
Windows Event Logs
W3C Logs
Syslog Messages
SNMP Traps Logs
Sql Server Audit
Oracle Audit
Edit filter...
< Back
Next >
Cancel

Screenshot 182 - Data filter dialog: Specifying data filter conditions

6. Specify which data will be filtered from your database backend. If no filter is specified, the selected maintenance job will affect all data within your database backend. Click **Next** to continue.

For more information on how to configure filter conditions, refer to Configuring data filter conditions in this manual.

New job wizard...
Completing the "New Job" Wizard
Select when the job should be executed:
Scheduled job
The job will be saved and executed according to the Enterprise Maintenance schedule options.
Run the job now
The job will be executed only once.
GFI
< Back
Finish
Cancel

Screenshot 183 - Specify when the job will be executed

7. Specify whether the selected maintenance job should be scheduled or executed immediately.

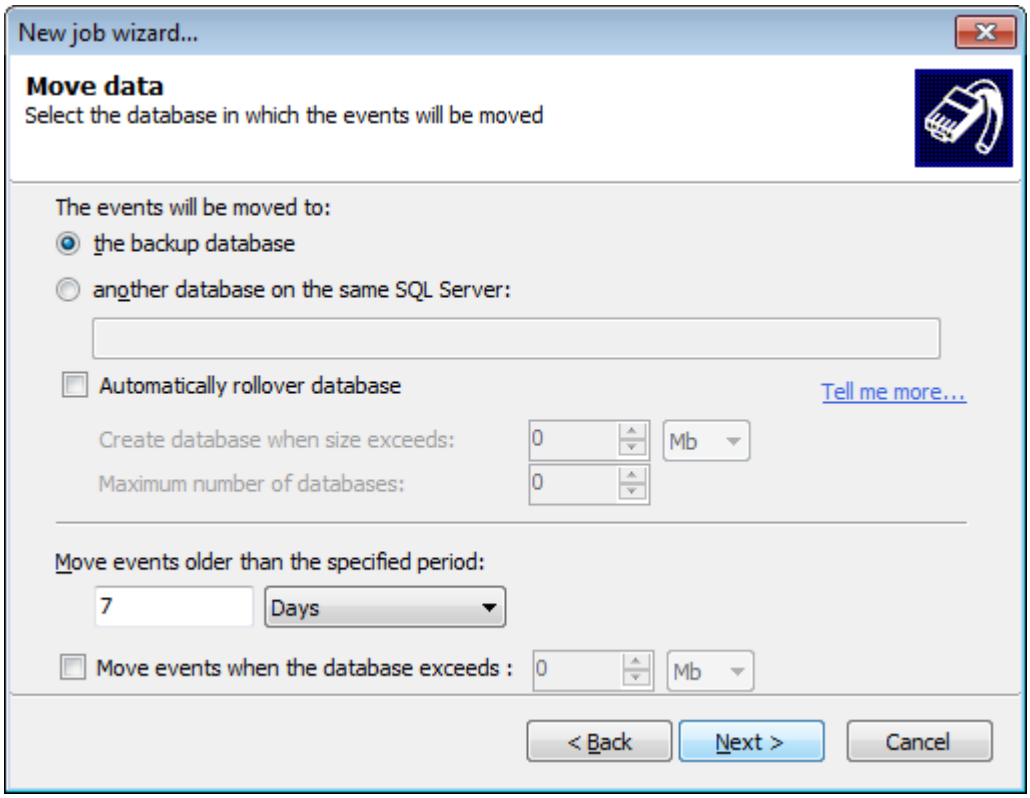
	Scheduled jobs are executed according to interval settings configured in the 'Database Operations'.
	Selected maintenance jobs will be executed only once.

8. Click **Finish** to finalize your configuration settings.

12.3.1 Move to database

To create a maintenance job that moves events between the main database and any other target database:

1. Launch the **'New job wizard'** dialog and select **Move to database** option.



Screenshot 184 - New job wizard: Move to database

2. Specify the database where events will be moved. This should either be the backup database or another accessible database on the SQL Server hosting the main database.

3. (Optional) Select **Automatically rollover database** to divide the data into multiple databases within the same SQL server. Configure the options described in Table 32 below.

Table 32 - Move to database - Rollover options

OPTIONS	DESCRIPTION
Create database when size exceeds:	Specify a valid database size. When the source database exceeds the specific size, a new database will be created.
Maximum number of databases:	Specify the maximum number of databases that can be created. If the number of maximum databases is exceeded, all events will be stored in the last created database.

4. Configure a valid time period in **Move events older than the specified period:** All events older than the configured value will be moved to the destination database.

5. (Optional) Select **Move events when the database exceeds:** and key in a valid size. Rollover will start when the source database reaches the configured size. If this option is

not selected, rollover will start when the source database reaches the size specified in **Create database when size exceeds:** in Step 3.

6. Click **Next**.

7. Configure the data filter conditions. If filtering conditions are not configured all events older than the specified period will be moved. Click **Next** to continue.

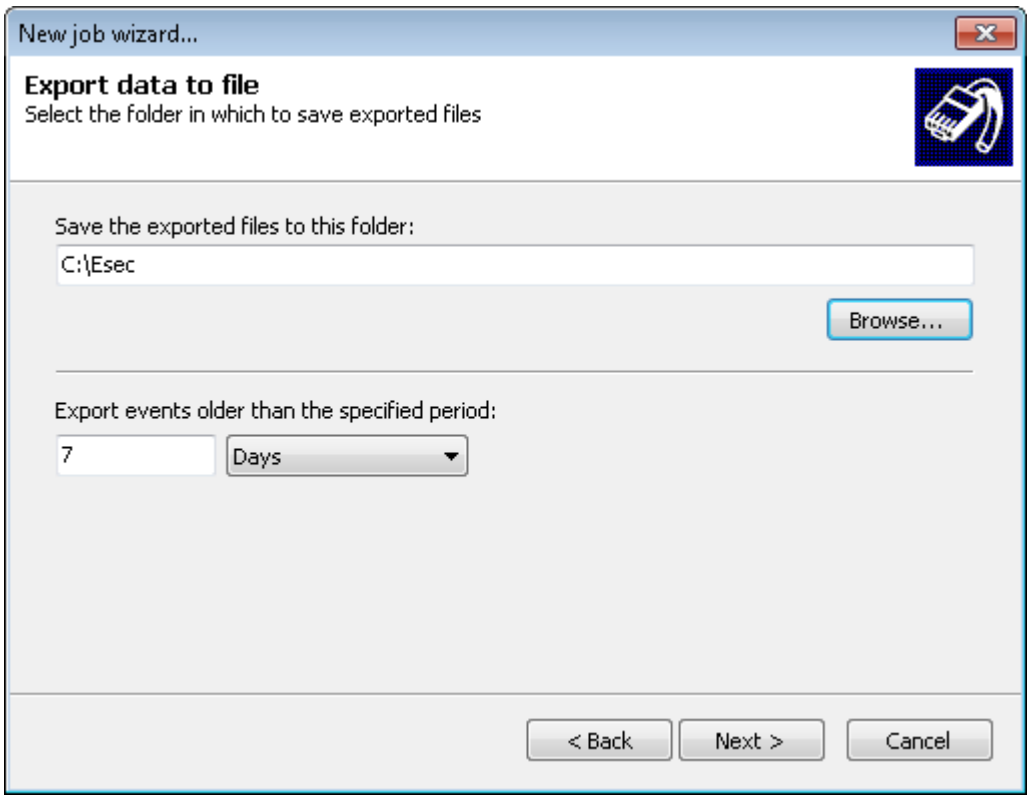
For more information on how to configure filter conditions, refer to Configuring data filter conditions section in this manual.

8. Specify whether the maintenance job should be scheduled or executed immediately and click **Finish**.

12.3.2 Export to file

To export events from the main database to a binary file:

1. Launch the 'New job wizard' and select the **Export to file** option.



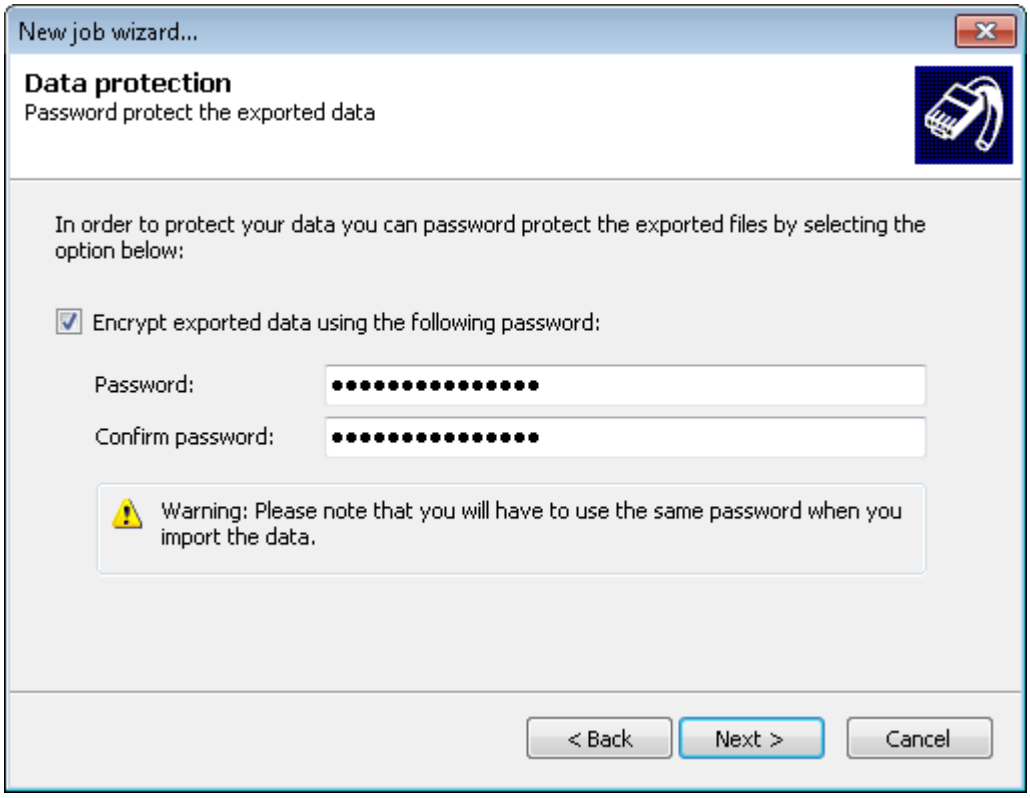
Screenshot 185 - New job wizard: Export to file

2. Specify the target folder where the exported file will be stored. Use the UNC notation to specify remote paths.

Ensure that GFI EventsManager has administrative privileges over the specified target folder.

3. Specify the frequency in hours/days at which events will be exported from the main database.

4. Click **Next**.


New job wizard...
Data protection
Password protect the exported data
In order to protect your data you can password protect the exported files by selecting the option below:
Encrypt exported data using the following password:
Password:
Confirm password:
Warning: Please note that you will have to use the same password when you import the data.
< Back
Next >
Cancel

Screenshot 186 - New job wizard: Export to file using encryption

5. Define whether the exported events data will be encrypted, specify the password to be used for decryption and click **Next** to proceed to the data filter dialog.

It is recommended that files to be exported are always encrypted using strong passwords.

6. Configure the data filter conditions that will be applied for 'Export to file' jobs. If you do not set any data filter conditions, than all events older than the specified period will be exported. Click **Next** to continue.

For more information on how to configure filter conditions, refer to Configuring data filter conditions section in this manual.

7. Define whether the maintenance job should be scheduled or executed immediately.

8. Click on **Finish** to finalize your settings.

Export filename

The convention used by GFI EventsManager to name the export file is shown and described below:

- **[ESM ID]_[Job ID]_[Date From]_[Date To].EXP**
- **ESM ID** - refers to the unique identifier given to each GFI EventsManager instance running in the organization.
- **Job ID** - refers to the unique identifier given to each maintenance job created.
- **Date From** - refers to the date of the earliest event exported.
- **Date To** - refers to the date of the latest event exported.
- **.EXP** - this is the file extension given to all export files.

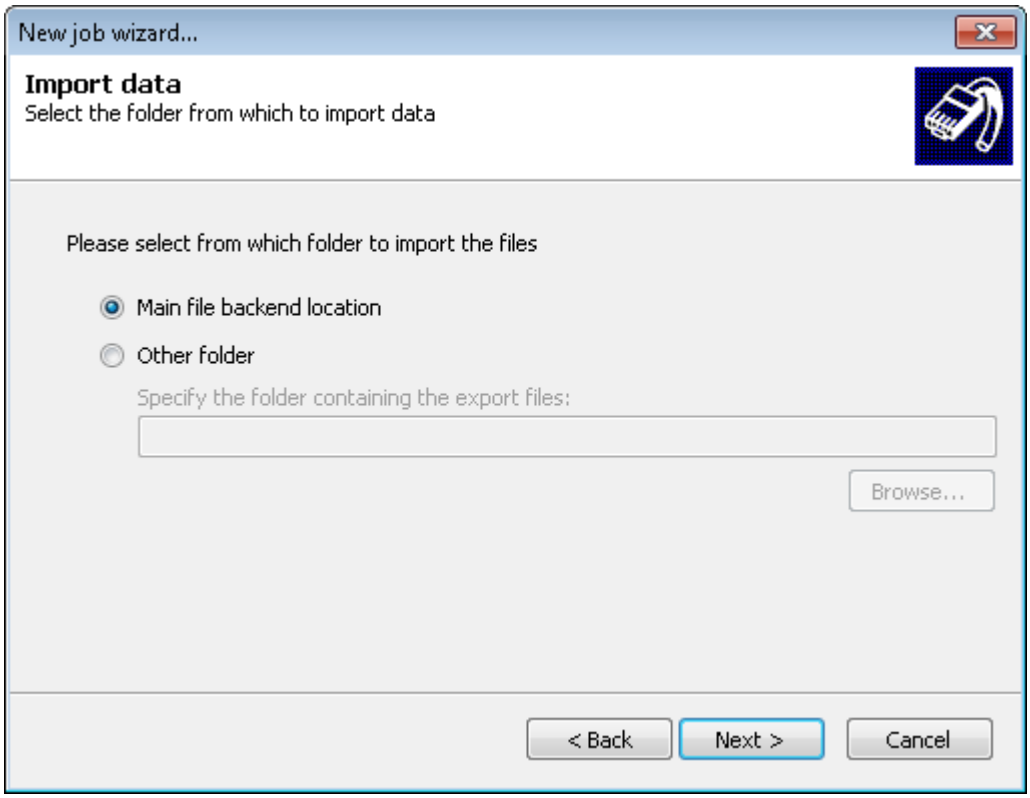
The following is an example of an export filename:

- **SERVER01_0051_20061020_20061025.EXP**

12.3.3 Import from file

To import events from a file or from the storage folder into the main database:

1. From **New job wizard** dialog, select **Import from file**.


New job wizard...
Import data
Select the folder from which to import data
Please select from which folder to import the files
Main file backend location
Other folder
Specify the folder containing the export files:
Browse...
< Back
Next >
Cancel

Screenshot 187 - New job wizard: Import from file

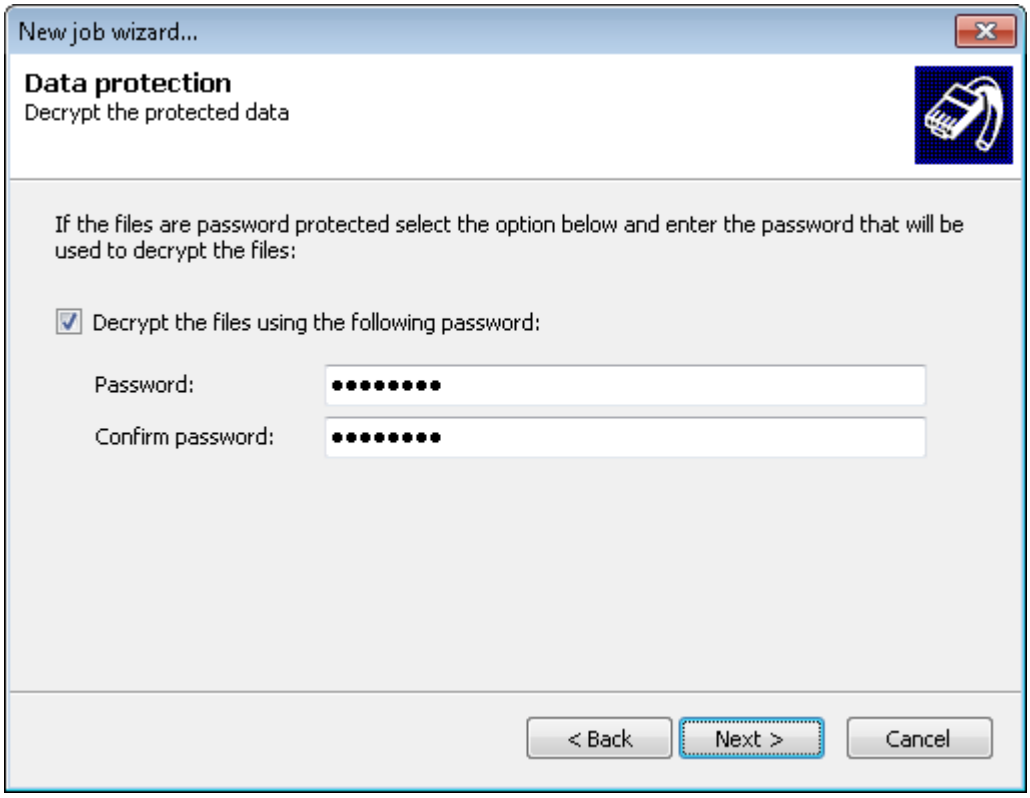
2. Specify from which folder to import the files. Select to import from:

» The main file backend. For more information on how to configure the storage folder, refer to .

» Other folder.

	Ensure that GFI EventsManager has administrative privileges over the specified folder.
	When **Other folder** is selected, GFI EventsManager will import all files having an EXP extension.

3. Click **Next** to proceed to the data protection dialog.


New job wizard...
Data protection
Decrypt the protected data
If the files are password protected select the option below and enter the password that will be used to decrypt the files:
Decrypt the files using the following password:
Password:
Confirm password:
< Back
Next >
Cancel

Screenshot 188 - New job wizard: Import from file decryption

4. Specify the password with which events data will be decrypted and click **Next** to proceed to the data filter dialog.

Use the same password used for the encryption of your events data.

Data encryption is not applicable when importing events from the storage folder.

5. Configure the data filters that will be applied against the imported file and click **Next** to continue.

Use data filters to define which events will be imported into the main database.

For more information on how to configure filter conditions, refer to Configuring data filter conditions section in this manual.

6. Specify whether the maintenance job should be scheduled or executed immediately.

7. Click on **Finish** to finalize settings.

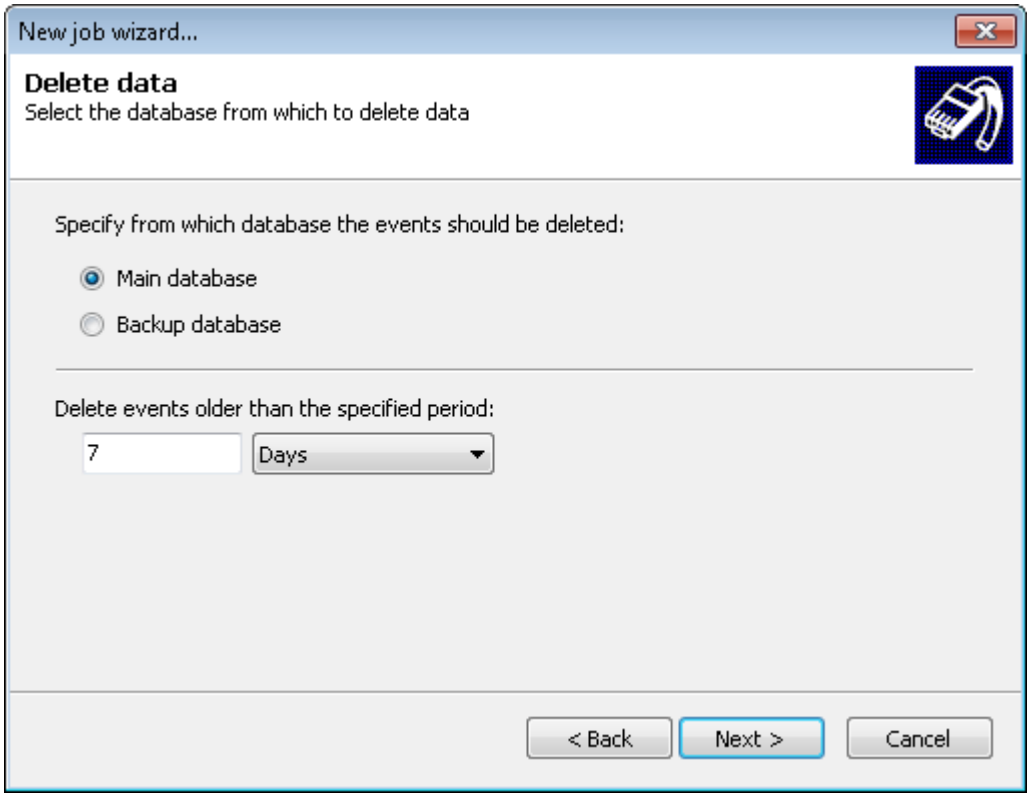
GFI EventsManager will change the file extension of all successfully imported files from .EXP to .IMP.

12.3.4 Delete data

To remove events from the main database:

1. From **New job wizard** dialog, select **Delete data**.

Important events should be backed up using **Move to database** or **Export to file** before deleting logs.



Screenshot 189 - New job wizard: Delete data

2. Specify whether events will be deleted from the Main database or from the Backup database.

3. Specify the frequency in hours/days at which events will be deleted from the main/backup database.

4. Click **Next**.

5. Configure the data filter conditions that will be applied for the 'Delete data' job. If you do not set any data filter conditions, than all events older than the specified period will be deleted. Click **Next** to continue.

For more information on how to configure filter conditions, refer to Configuring data filter conditions in this manual.

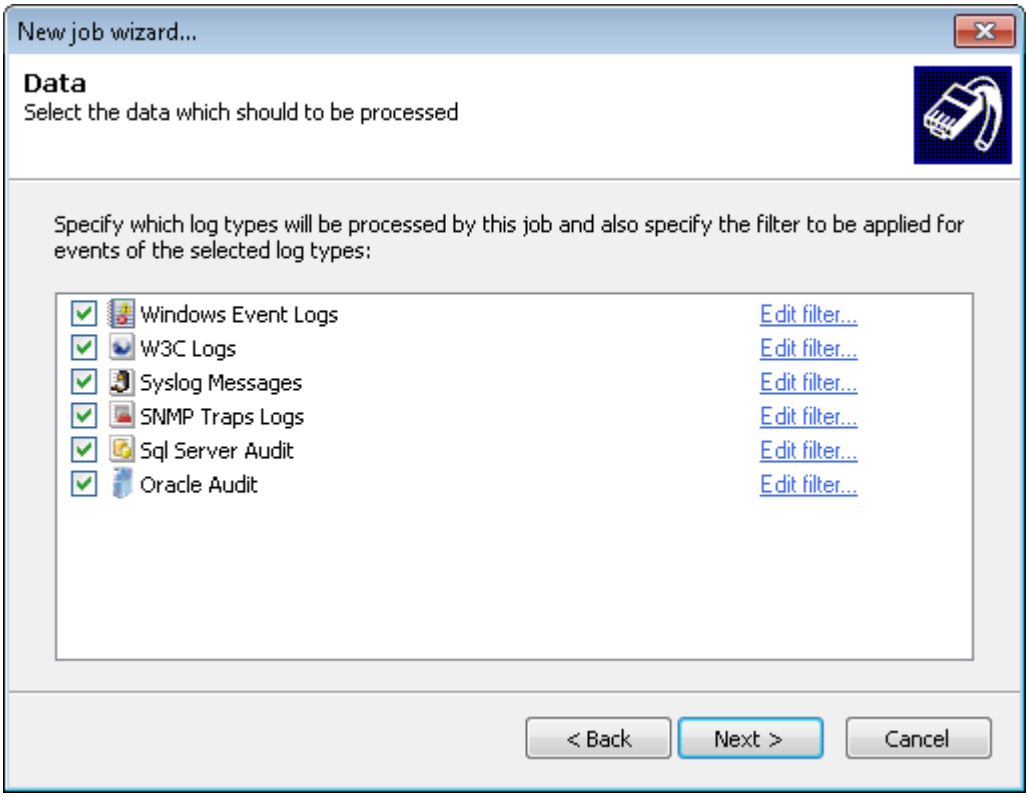
6. Specify whether the maintenance job should be scheduled or executed immediately.

7. Click **Finish**.

12.3.5 Configuring data filter conditions

Use data filter conditions to specify which events will be affected by the maintenance job. Only events which match the specified criteria will be processed, moved, exported, deleted or imported.

Filters can be created for all log types supported by GFI EventsManager.



Screenshot 190 - Data filter dialog

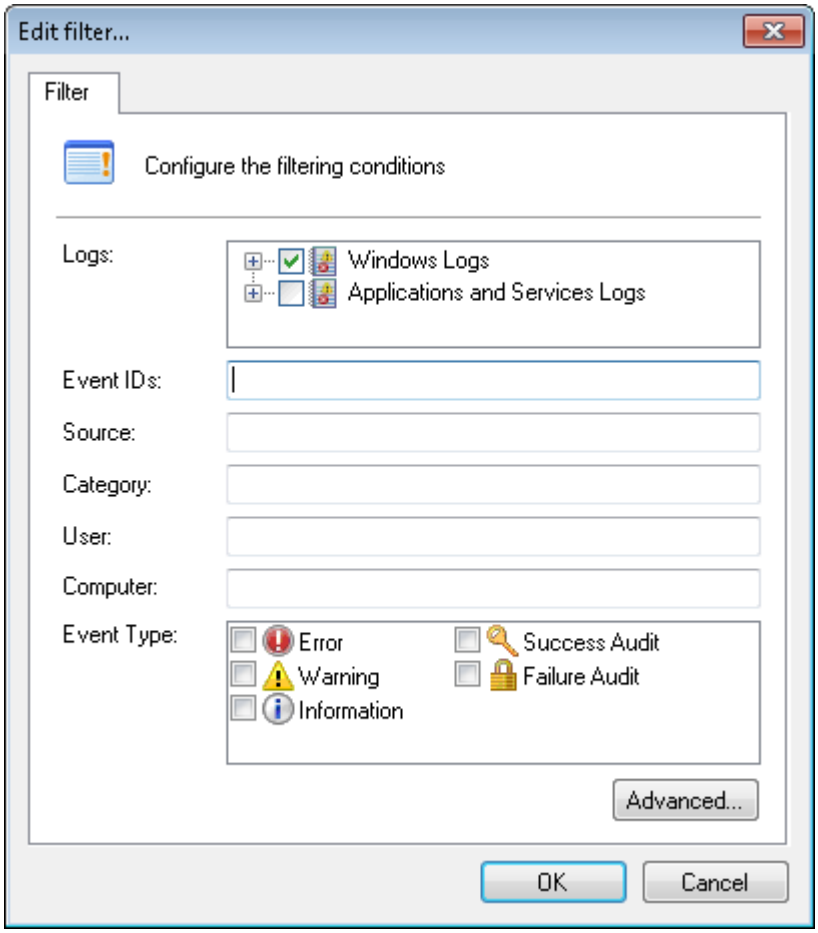
To specify which events are affected by maintenance jobs, click **Filter** button in the data filter dialog. This dialog is available through the 'New job wizard'.

Example: Windows Event Log filter

Export events from the Windows Event Log with the following conditions:

- **Log type**: Security
- **Event ID**: 540 - Successful logon
- **User**: administrator
- Event Type: Error.

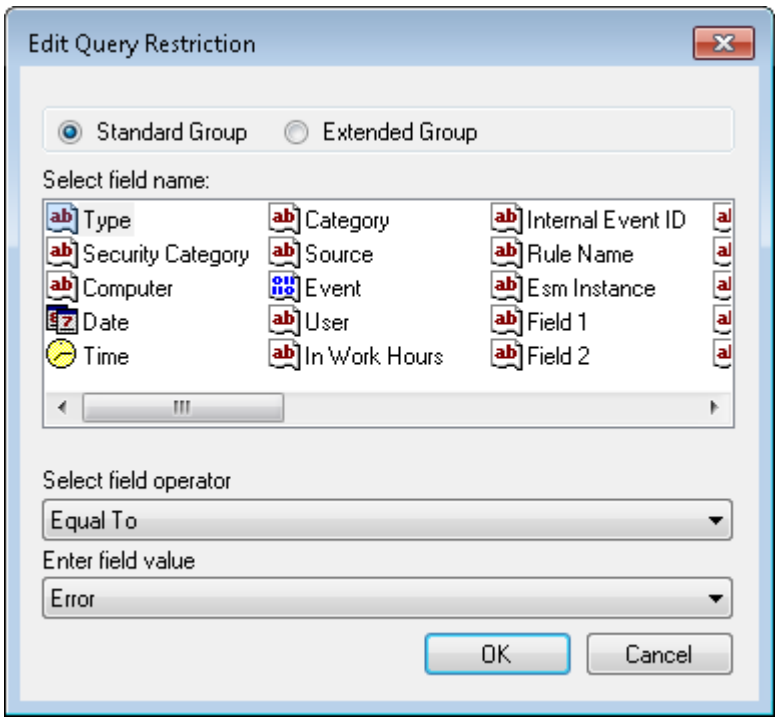
Configure your filter parameters as shown in the 'Edit filter' dialog shown below:



Screenshot 191 - Creating a filter for Windows events: Edit filter dialog

Click **Ok** to finalize filter configuration.

Advanced conditions



Screenshot 192 - Advanced Filter settings

From the **Edit filter** dialog you can also set advanced filter conditions. Through this dialog you can also create and apply filters on all events data fields used by GFI EventsManager.

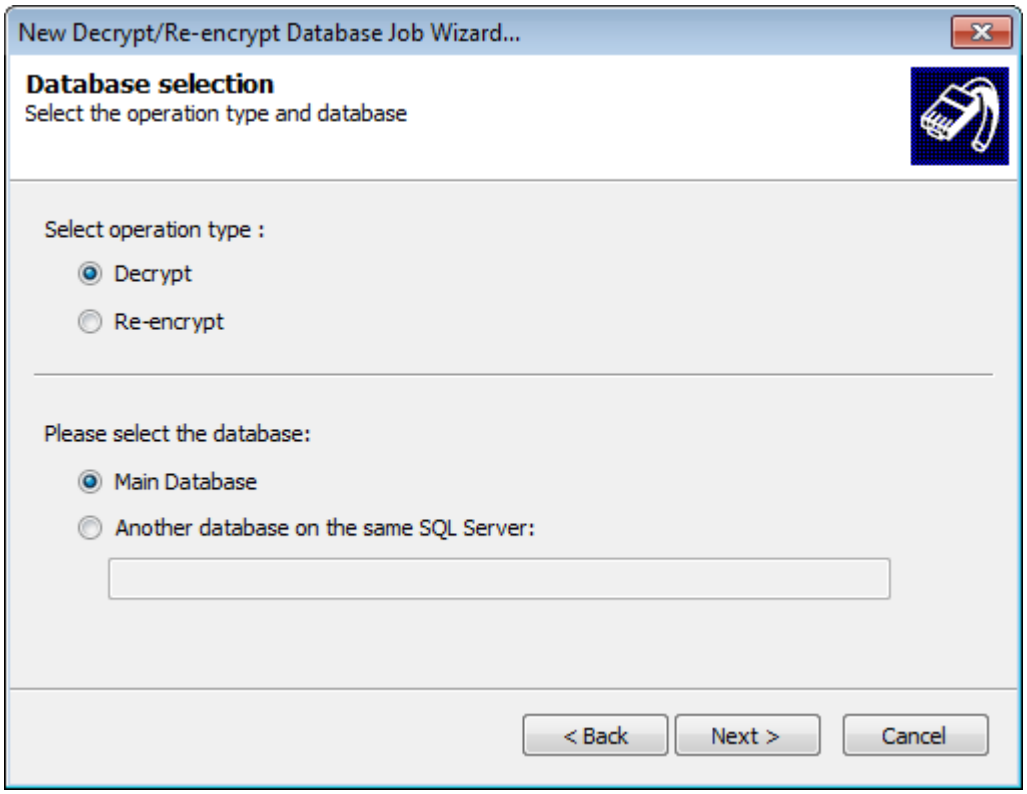
Filters can also be applied on maintenance jobs after they have been created. For more information refer to Edit existing maintenance jobs section.

12.4 Create new anonymization job

When anonymization is enabled, events stored in the central database are encrypted.

To decrypt /re-encrypt events stored in the central database:

1. From **Configuration** tab, click **Options**.
2. Click **Database Operations** and select **Create new anonymization job…**
3. Click **Next**.

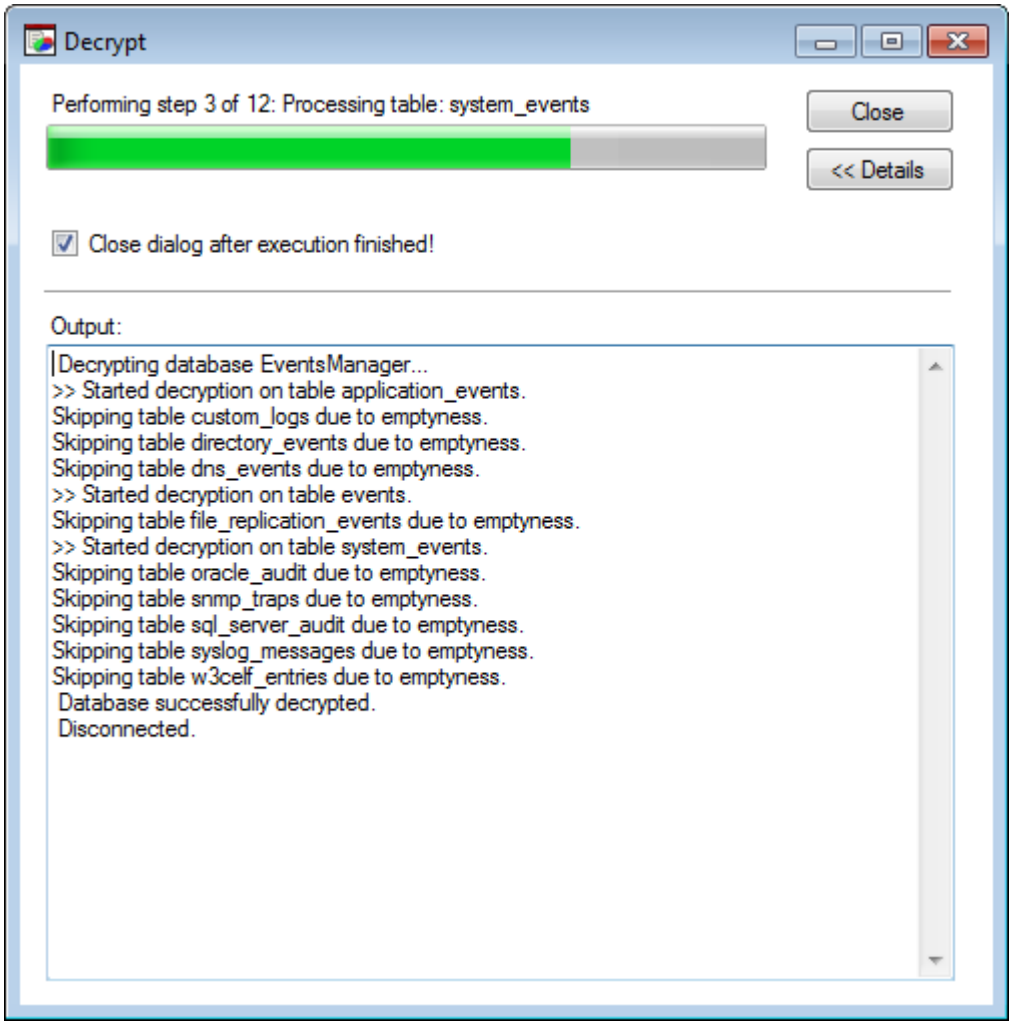


Screenshot 193 - New Decrypt/Re-encrypt database job wizard

4. Select **Decrypt** or **Re-encrypt** to decrypt or encrypt the event logs respectively.
5. Select the database. Click **Next**.
6. Specify the decryption/re-encryption password. Click **Next**.

If **Use a secondary protection key** was selected when encrypting the database, select **Use secondary decryption key** and specify the password. Click **Next**. For information on how to enable anonymization, refer to Anonymization section in this manual.

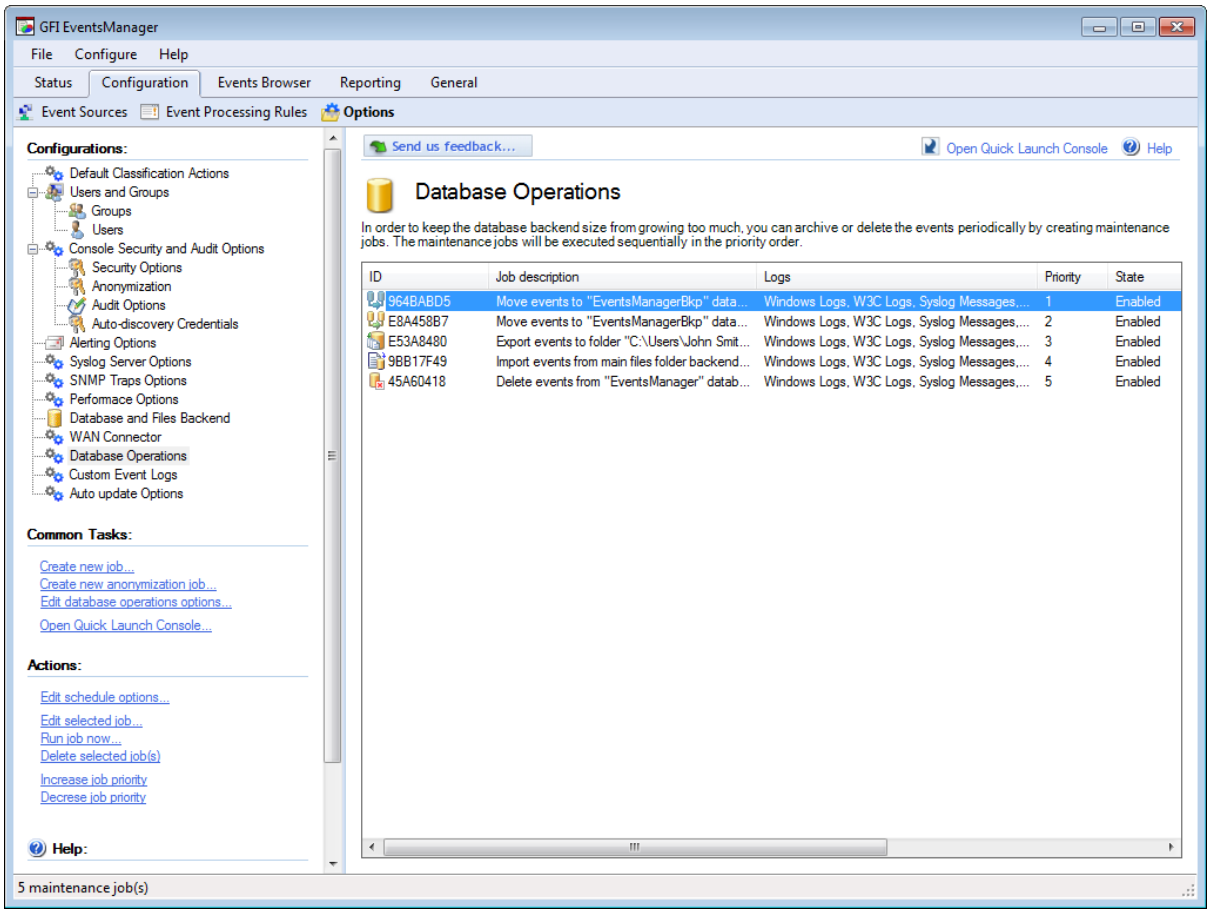
7. Click **Finish** to start the job.



Screenshot 194 - New anonymization job progress

Once the job is completed, event logs stored in the central database can be viewed from the **Events Browser**, **Dashboard** and reports.

12.5 Edit existing maintenance jobs


GFI EventsManager
File Configure Help
Status Configuration Events Browser Reporting General
Event Sources Event Processing Rules Options
Configurations:
Default Classification Actions
Users and Groups
Groups
Users
Console Security and Audit Options
Security Options
Anonymization
Audit Options
Auto-discovery Credentials
Alerting Options
Syslog Server Options
SNMP Traps Options
Performace Options
Database and Files Backend
WAN Connector
Database Operations
Custom Event Logs
Auto update Options
Common Tasks:
Create new job...
Create new anonymization job...
Edit database operations options...
Open Quick Launch Console...
Actions:
Edit schedule options...
Edit selected job...
Run job now...
Delete selected job(s)
Increase job priority
Decrese job priority
Help:
Send us feedback...
Open Quick Launch Console
Help
Database Operations
In order to keep the database backend size from growing too much, you can archive or delete the events periodically by creating maintenance jobs. The maintenance jobs will be executed sequentially in the priority order.
ID
Job description
Logs
Priority
State
964BABD5 Move events to "EventsManagerBkp" data... Windows Logs, W3C Logs, Syslog Messages,... 1 Enabled
E8A458B7 Move events to "EventsManagerBkp" data... Windows Logs, W3C Logs, Syslog Messages,... 2 Enabled
E53A8480 Export events to folder "C:\Users\John Smit... Windows Logs, W3C Logs, Syslog Messages,... 3 Enabled
9BB17F49 Import events from main files folder backend... Windows Logs, W3C Logs, Syslog Messages,... 4 Enabled
45A60418 Delete events from "EventsManager" datab... Windows Logs, W3C Logs, Syslog Messages,... 5 Enabled
5 maintenance job(s)

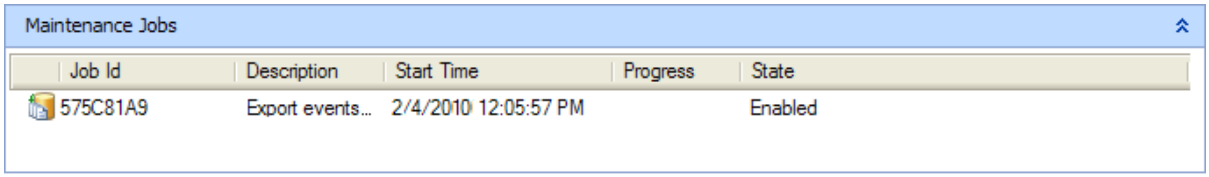
Screenshot 195 - Viewing scheduled maintenance jobs

To view maintenance jobs created:

1. Click **Configuration** tab and select **Options**.

2. From the left pane, select the **Database Operations** node. Scheduled maintenance jobs will be displayed in the right pane.

Job activity status



Screenshot 196 - Job activity status

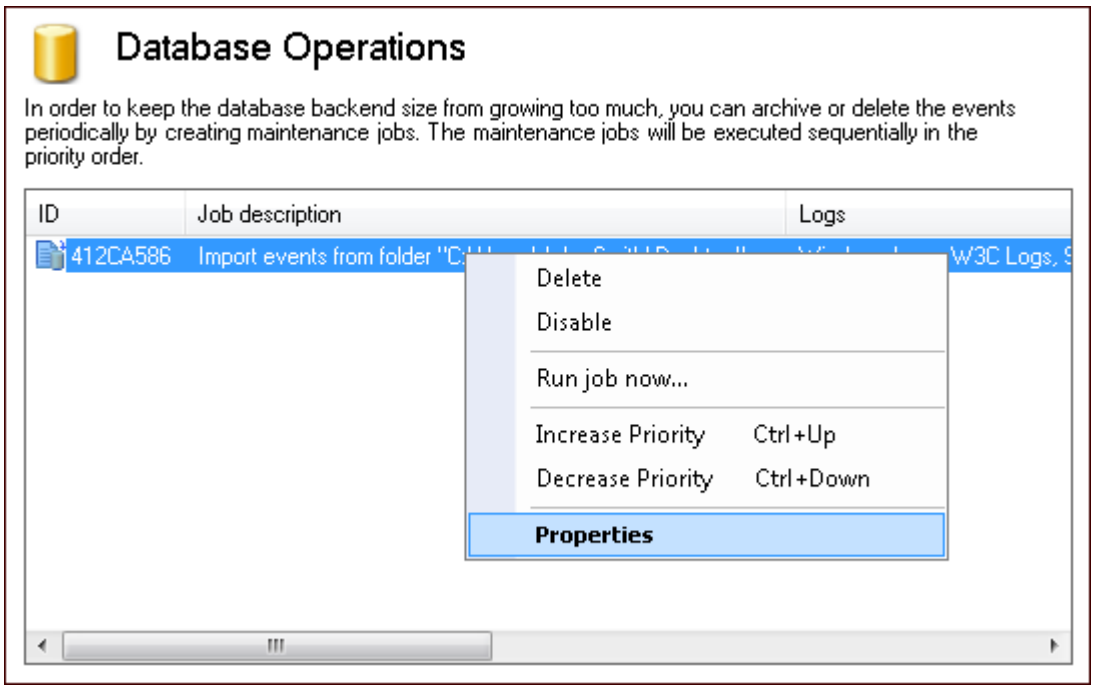
To view the progress of maintenance jobs that are being processed click **Status** tab and select the **Job Activity** dashboard view. The status of all maintenance jobs will be displayed in the **Maintenance Jobs** section.

You can make changes to maintenance job parameters for jobs scheduled.

1. Click **Configuration** tab and select **Options**.

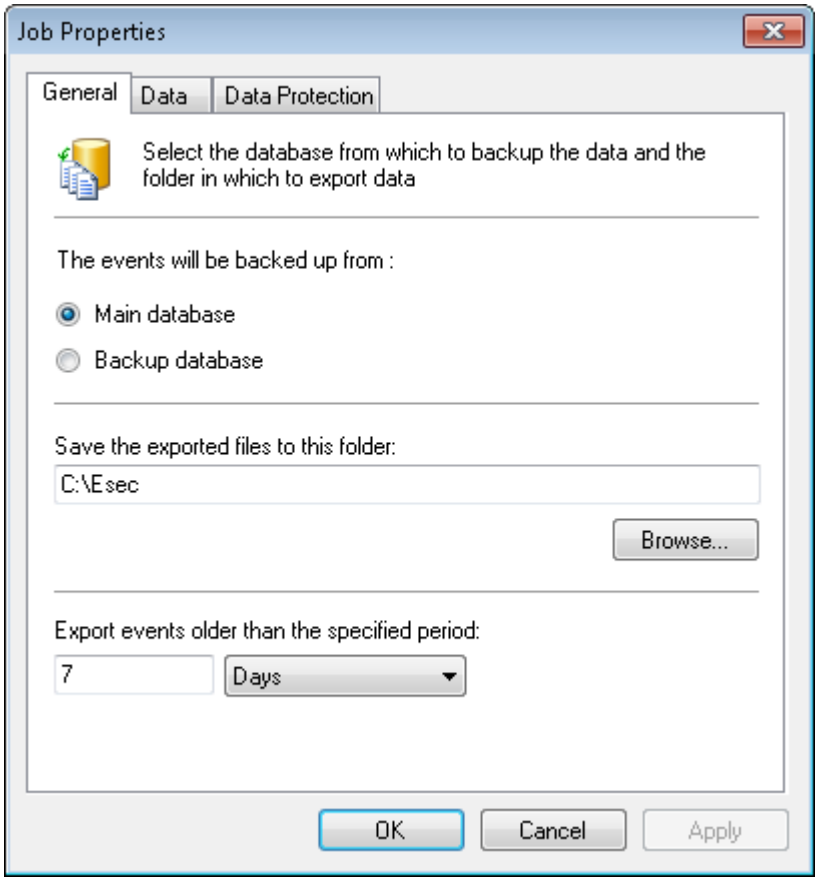
2. From the left pane, select the **Database Operations** node.

3. From the right pane, right-click maintenance job to edit and select **Properties**.


Database Operations
In order to keep the database backend size from growing too much, you can archive or delete the events periodically by creating maintenance jobs. The maintenance jobs will be executed sequentially in the priority order.
ID
Job description
Logs
412CA586
Import events from folder
Delete
Disable
Run job now...
Increase Priority Ctrl+Up
Decrease Priority Ctrl+Down
Properties

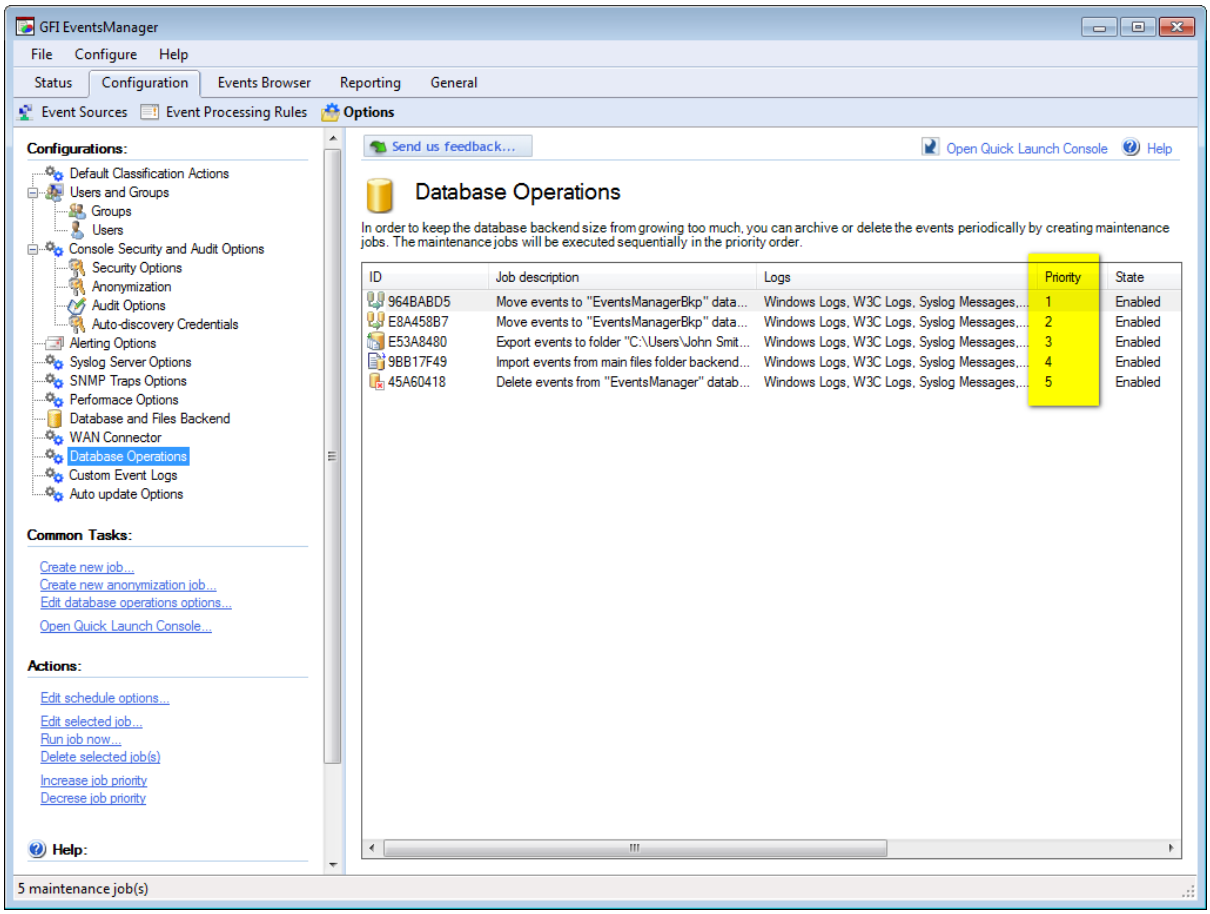
Screenshot 197 - Editing a maintenance job

4. Configure job properties and click **OK** to finalize your settings.



Screenshot 198 - Example dialog to edit a scheduled job

12.5.1 Changing maintenance job priority



Screenshot 199 - Maintenance job priorities

By default maintenance jobs are executed according to the sequence with which the jobs are created (First-in-First-out). Thus the priority of maintenance jobs is determined by the sequence in which jobs are executed.

To increase or decrease the priority of a maintenance job:

1. Click **Configuration** tab and select **Options**.

2. From the left pane, select the **Database Operations** node.

3. From the right pane, right-click the maintenance job and select **Increase Priority** or **Decrease Priority** accordingly.

12.5.2 Deleting a maintenance job

Scheduled maintenance jobs awaiting execution can also be deleted.

1. Click **Configuration** tab and select **Options**.

2. From the left pane, select the **Database Operations** node.

3. From the right pane, right-click on the maintenance job to delete and select **Delete**.

Before deleting maintenance jobs ensure that before deleting data, all data is backed up.

13.1 Enabling permissions on event sources manually

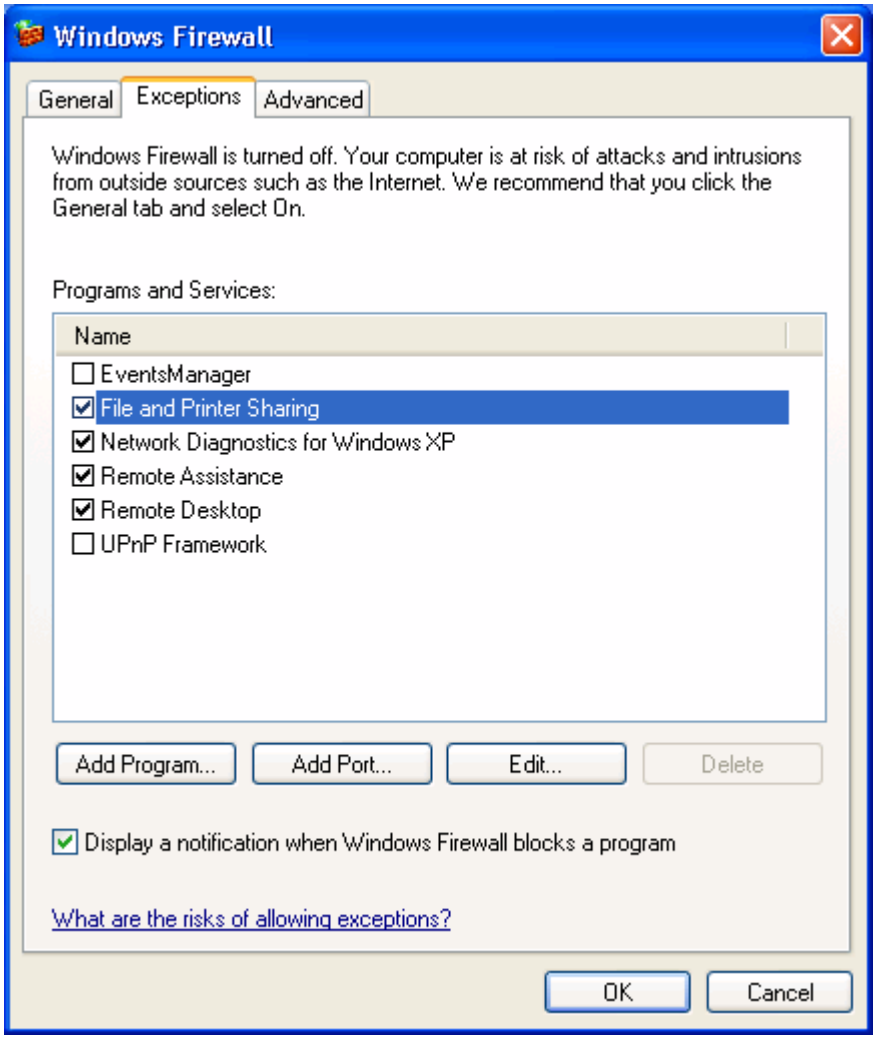
This section describes how to configure permissions and ports that are required by GFI EventsManager manually. This process has to be done on each machine to scan.

In a Windows 2003 or 2008 Active Directory environment, settings can be deployed automatically via Group Policy Object (GPO). For more information refer to Setting permissions on target computers automatically via GPO.

13.1.1 Microsoft Windows XP

To enable permissions and open the required ports on Microsoft Windows XP target machines:

1. Click **Start** ► **Control Panel** ► **Windows Firewall** ► **Exceptions** tab.



Screenshot 200 - Firewall rules on Microsoft Windows XP

2. Enable **File and Printer Sharing** from the **Programs and Services** list.

3. Click **OK** to apply changes and close.

13.1.2 Microsoft Windows Vista

Step 1: Enable Firewall permissions

To manually enable firewall rules on Microsoft Windows Vista:

1. Click **Start** ► **Control Panel** ► **Security** and click **Allow a program through Windows Firewall** from the left panel.

2. Select **Exceptions** tab and from **Allowed programs and features** list, enable the following rules:

» Remote Event Log Management

» File and Printer Sharing

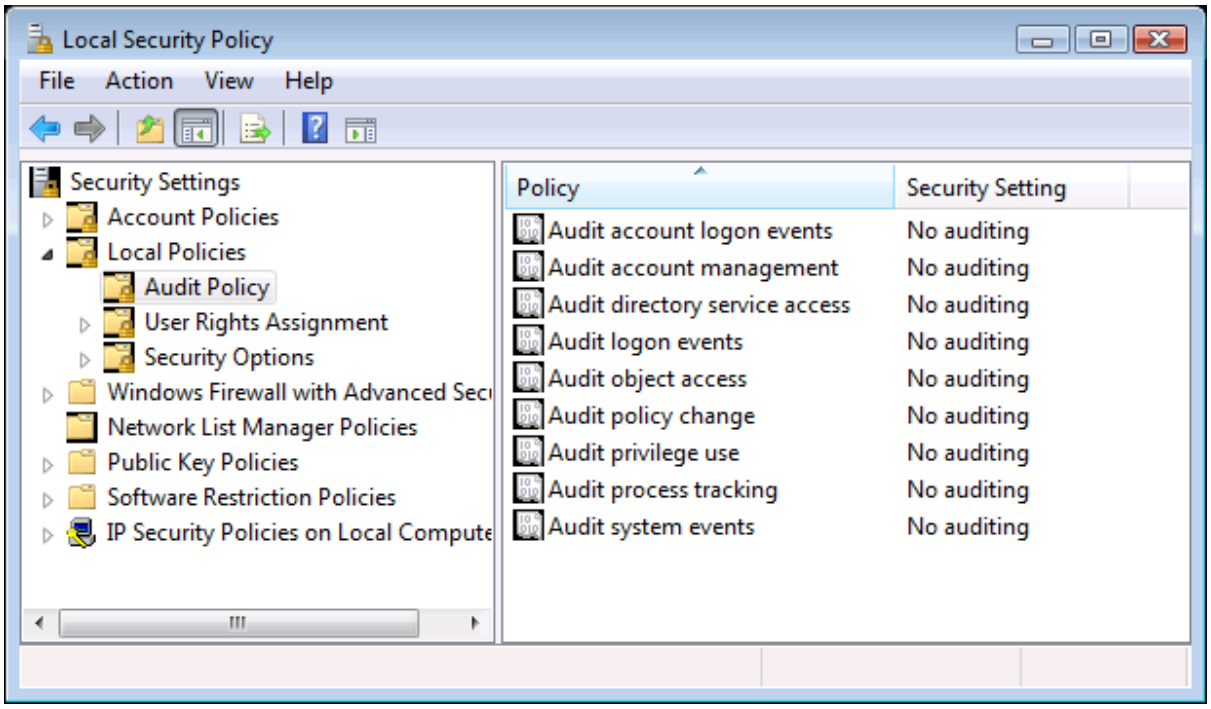
» Network Discovery

3. Click **Apply** to apply changes.

Step 2: Enable additional auditing features

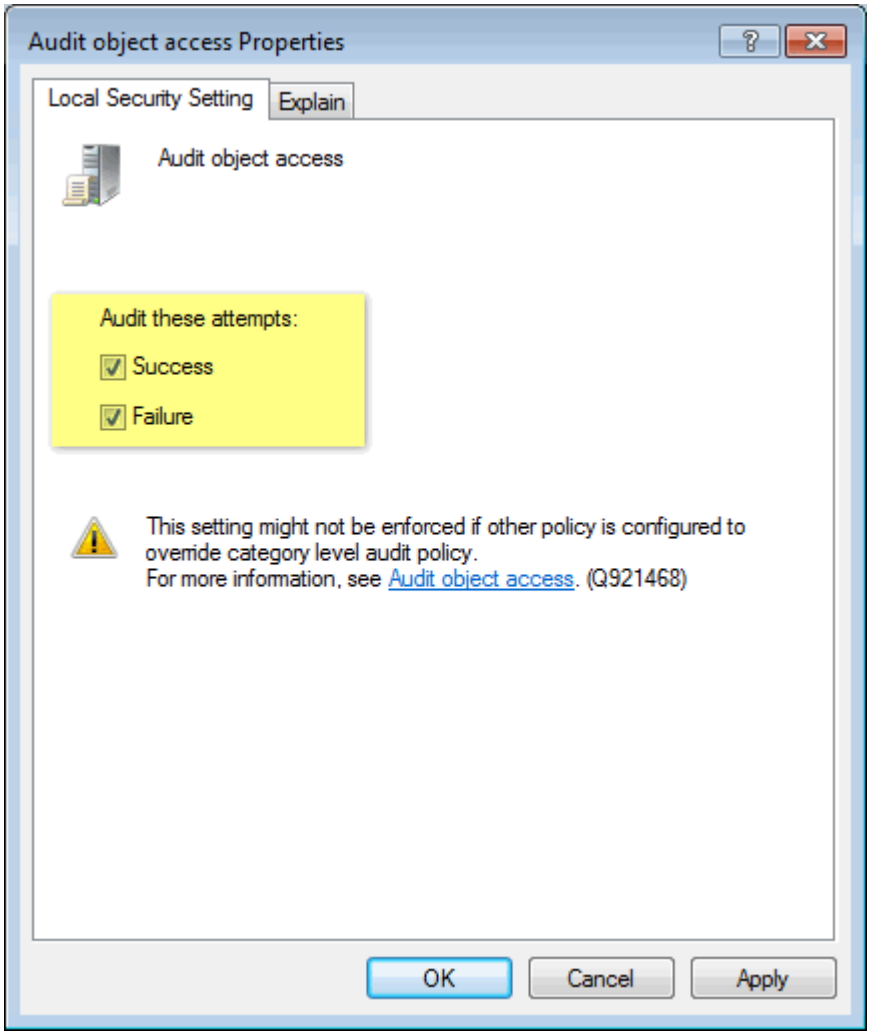
1. From a command prompt key in **secpol.msc** and press **Enter**.

2. From the **Security Settings** node, expand **Local Policies** ► **Audit Policy**.



Screenshot 201 - Local security policy window

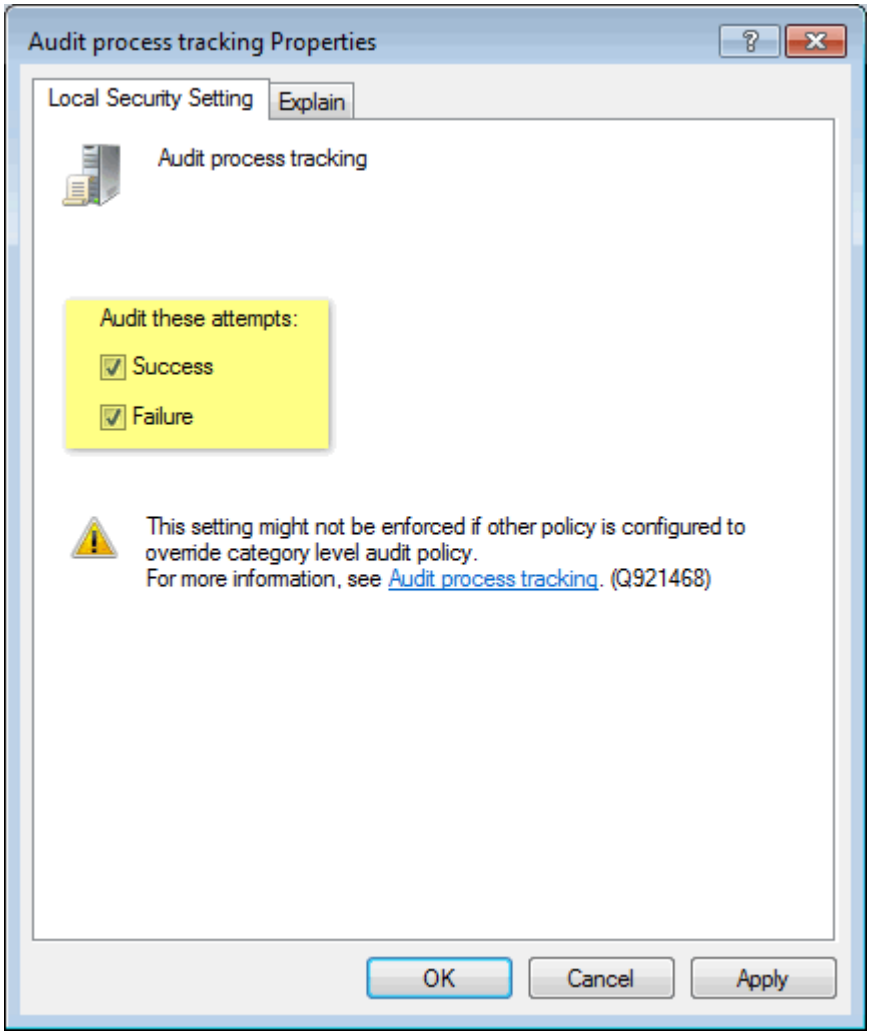
3. From the right panel, double click **Audit object access**.



Screenshot 202 - Audit object access Properties

4. From the **Audit object access Properties**, select **Success** and **Failure** and click **OK**.

5. From the right panel, double click **Audit Process tracking**.

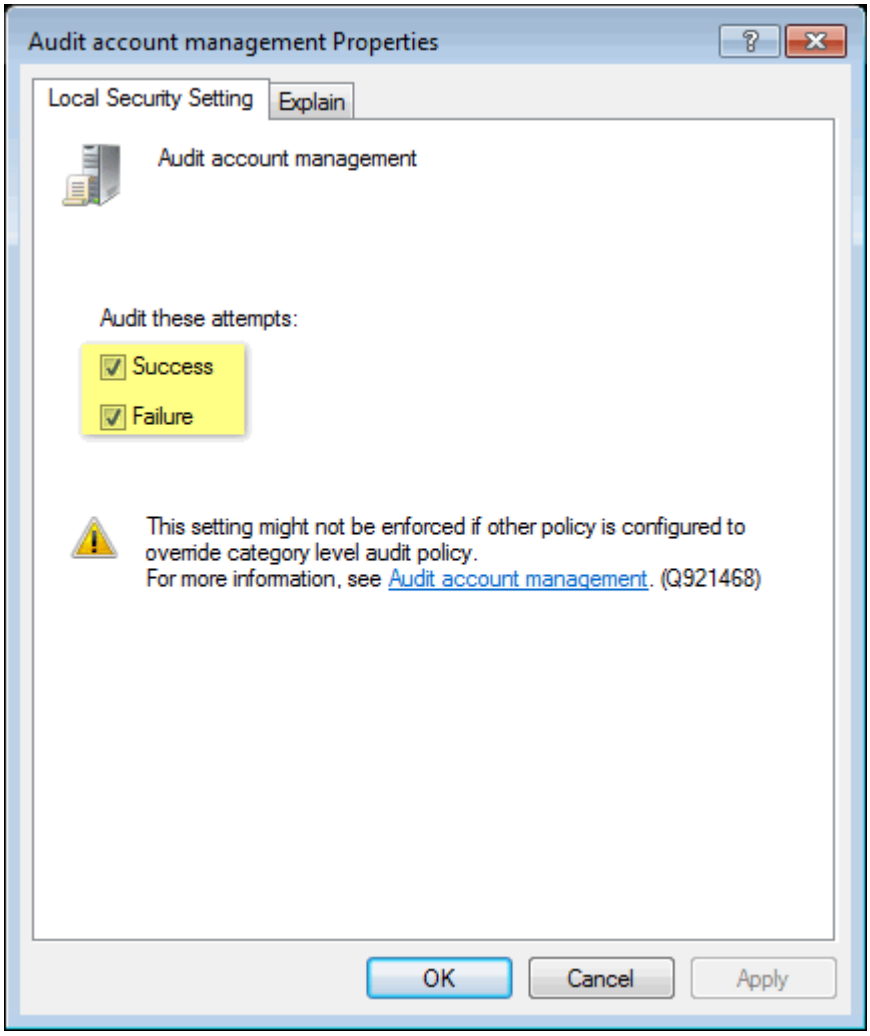


Screenshot 203 - Audit process tracking Properties

6. From the **Audit process tracking Properties**, select **Success** and **Failure** and click **OK**.

7. From the right panel, double click **Audit account management**.

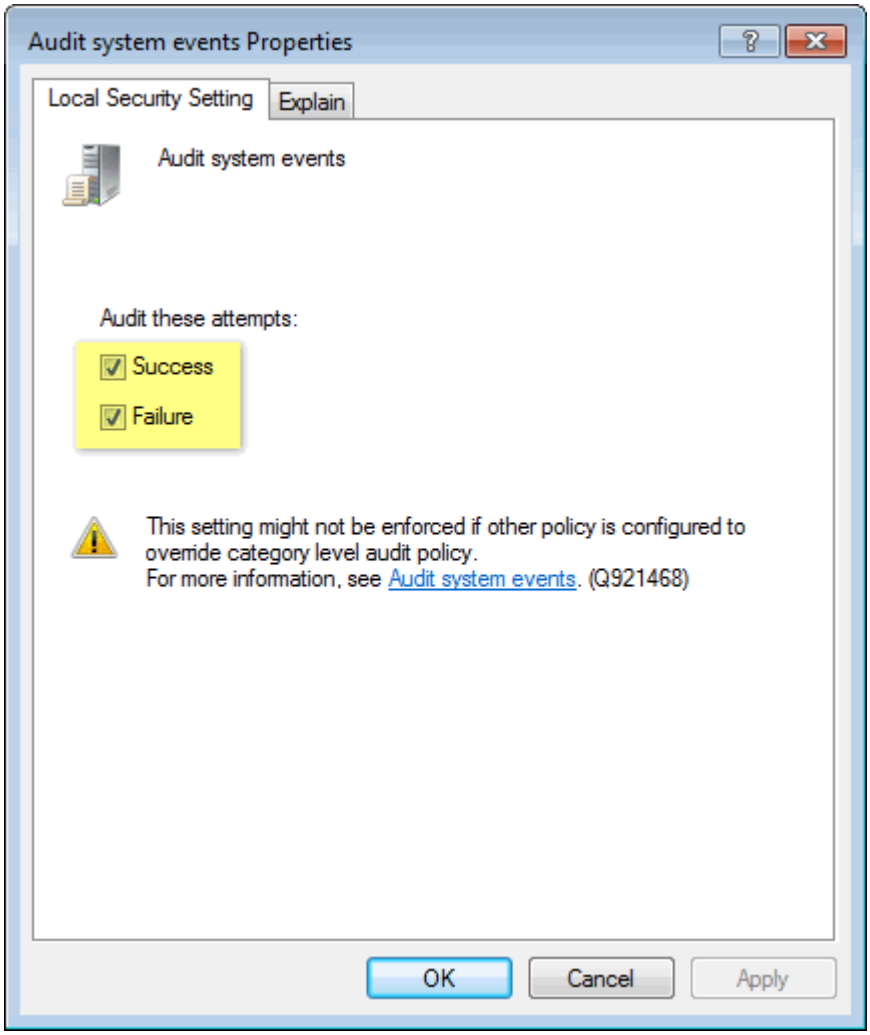
8. From the **Audit process tracking Properties**, select **Success** and **Failure** and click **OK**.



Screenshot 204 - Audit account management properties

9. From the right panel, double click **Audit system events**.

10. From the **Audit process tracking Properties**, select **Success** and **Failure** and click **OK**.



Screenshot 205 - Audit system events properties

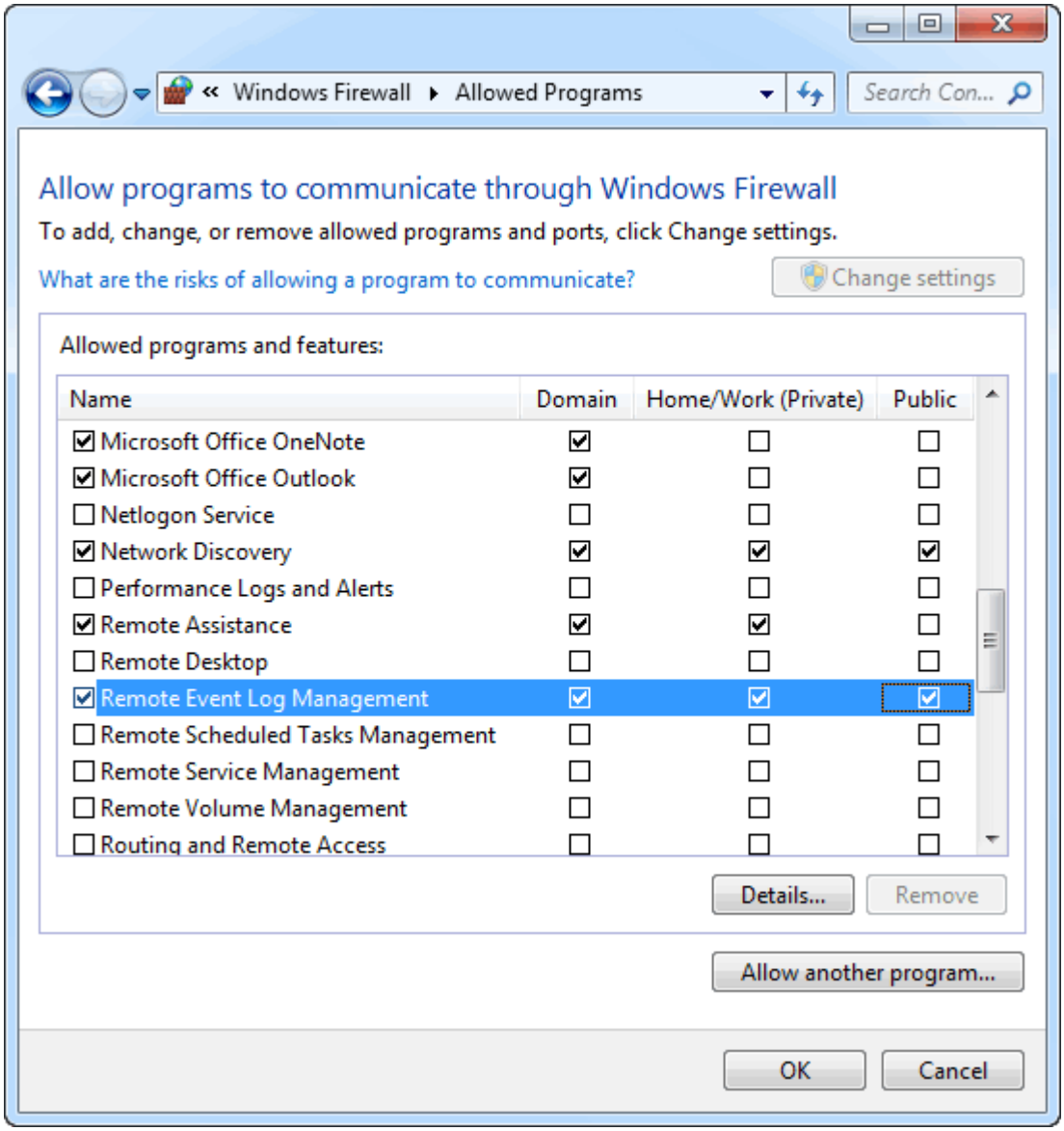
11. Close the **Local Security Policy** window.

13.1.3 Microsoft Windows 7

Step 1: Enable Firewall permissions

To manually enable firewall rules on Microsoft Windows 7:

1. Click **Start ► Control Panel ► System and Security** and click **Allow a program through Windows Firewall**, under **Windows Firewall** category.



Screenshot 206 - Allowed programs in Microsoft Windows Vista or later

2. From **Allowed programs and features** list, enable the following rules:

» Remote Event Log Management

» File and Printer Sharing

» Network Discovery

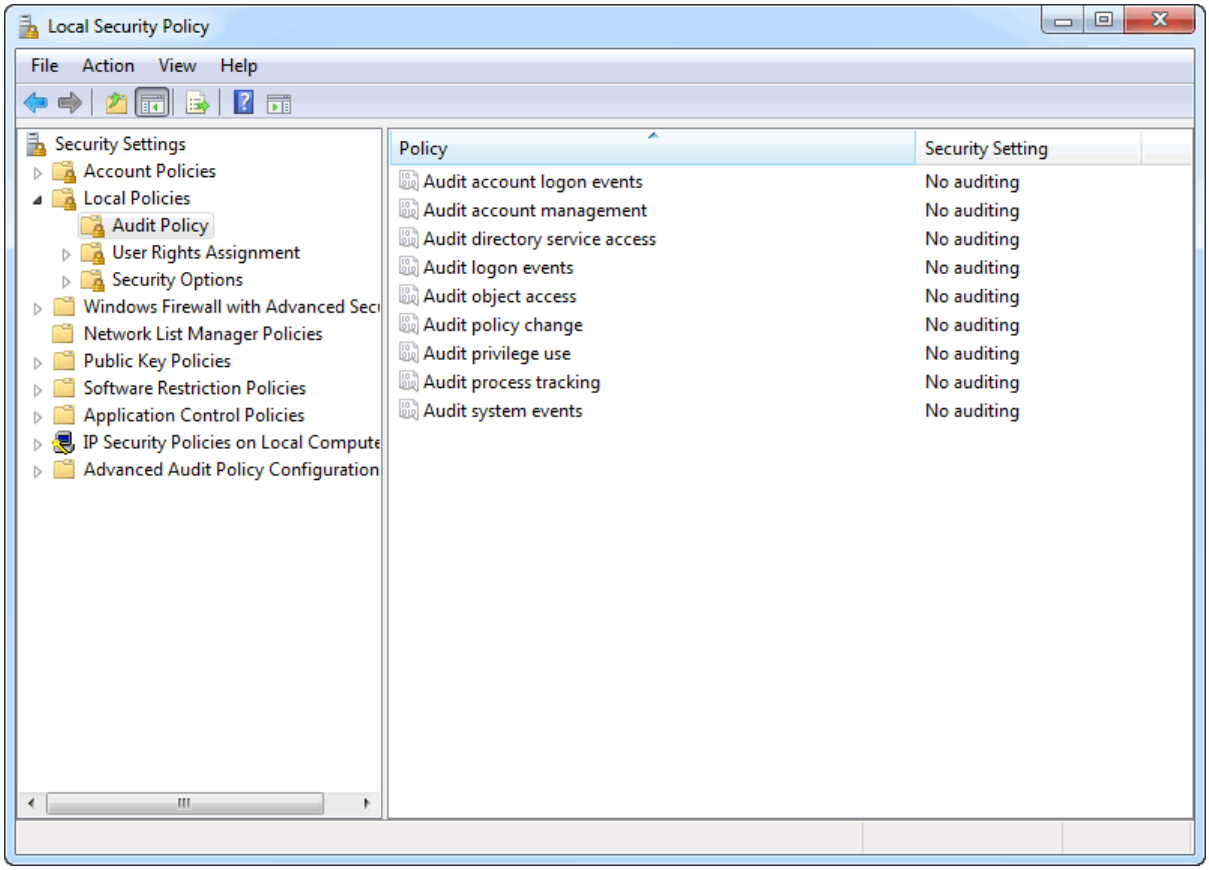
3. Select **Domain**, **Private** and **Public** for each rule mentioned above.

4. Click **OK** to apply changes.

Step 2: Enable additional auditing features

1. From command prompt key in **secpol.msc** and press **Enter**.

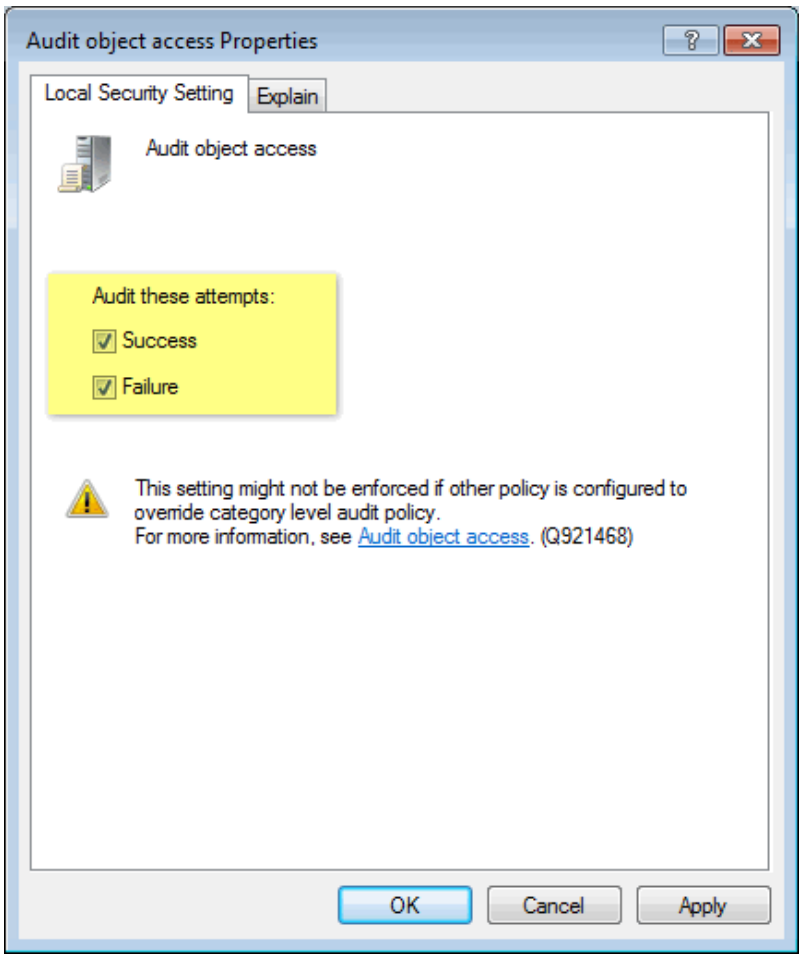
2. From the **Security Settings** node, expand **Local Policies ► Audit Policy**.



Screenshot 207 - Local security policy window

3. From the right panel, double click **Audit object access**.

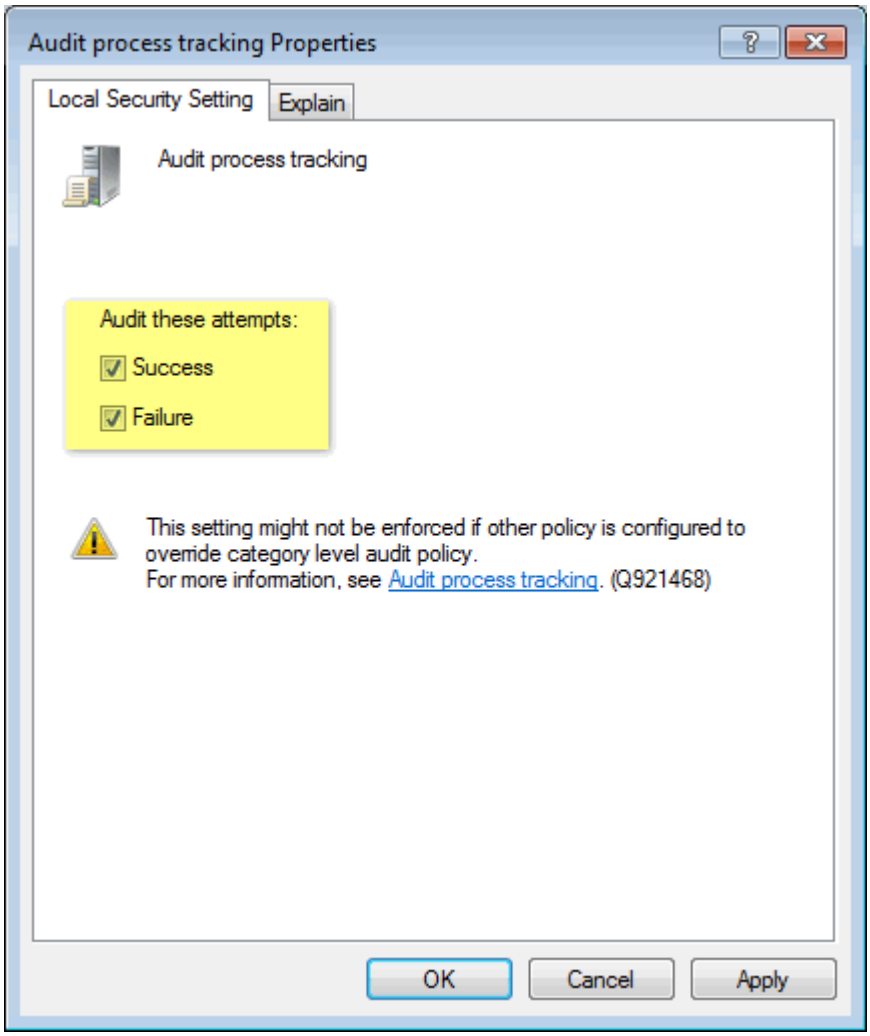
4. From the **Audit object access Properties**, select **Success** and **Failure** and click **OK**.



Screenshot 208 - Audit object access Properties

5. From the right pane, double click **Audit Process tracking.**

6. From the **Audit process tracking Properties**, select **Success** and **Failure** and click **OK.**

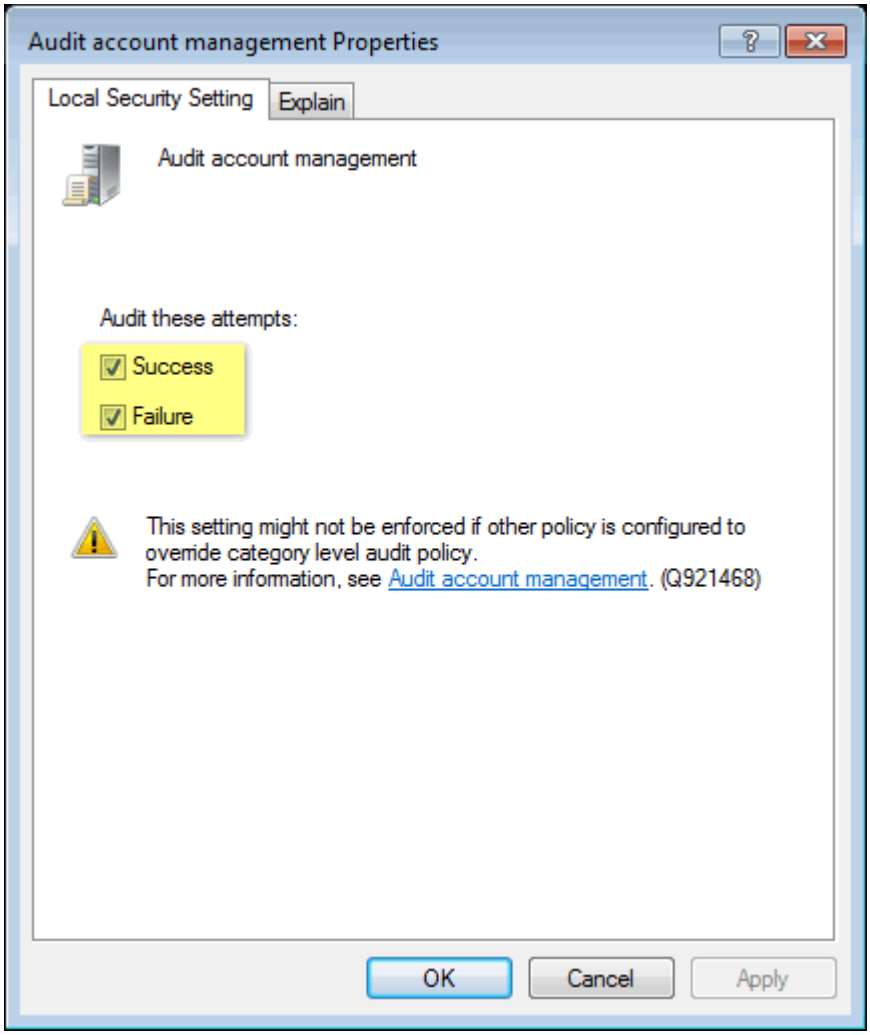


Screenshot 209 - Audit process tracking Properties

7. From the **Audit process tracking Properties**, select **Success** and **Failure** and click **OK.**

8. From the right panel, double click **Audit account management.**

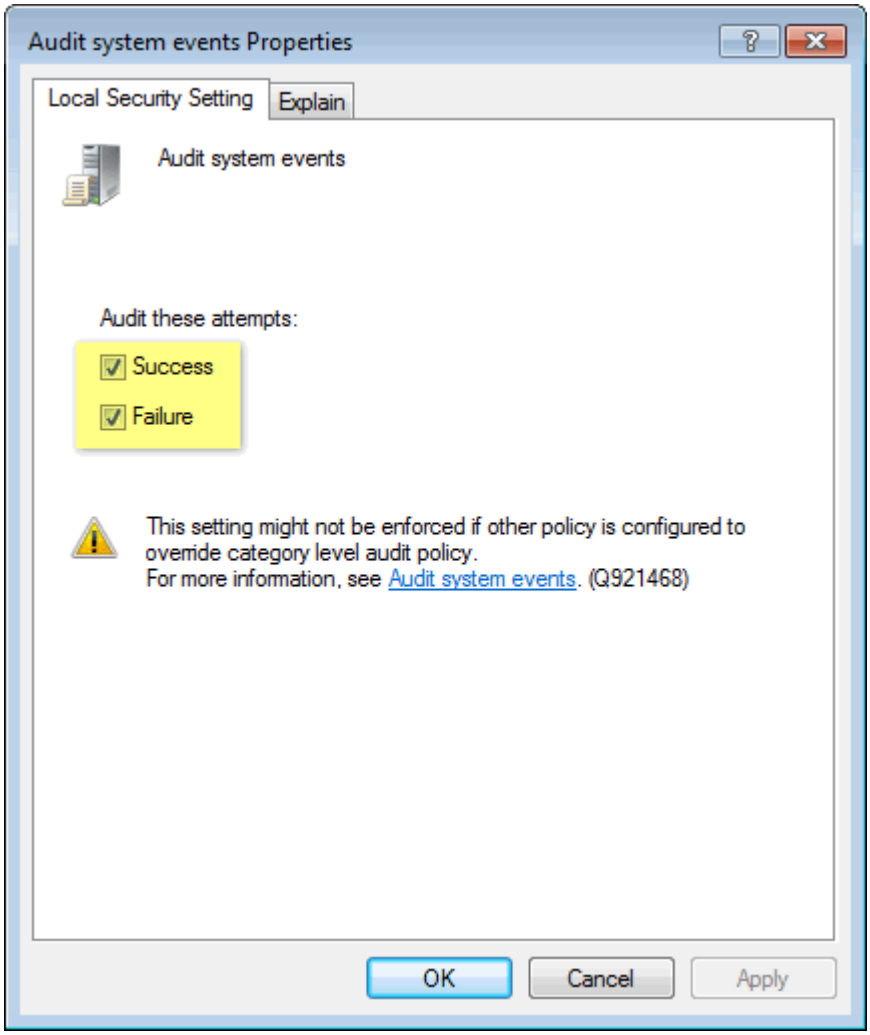
9. From the **Audit process tracking Properties**, select **Success** and **Failure** and click **OK.**



Screenshot 210 - Audit account management properties

10. From the right panel, double click **Audit system events**.

11. From the **Audit process tracking Properties**, select **Success** and **Failure** and click **OK**.



Screenshot 211 - Audit system events properties

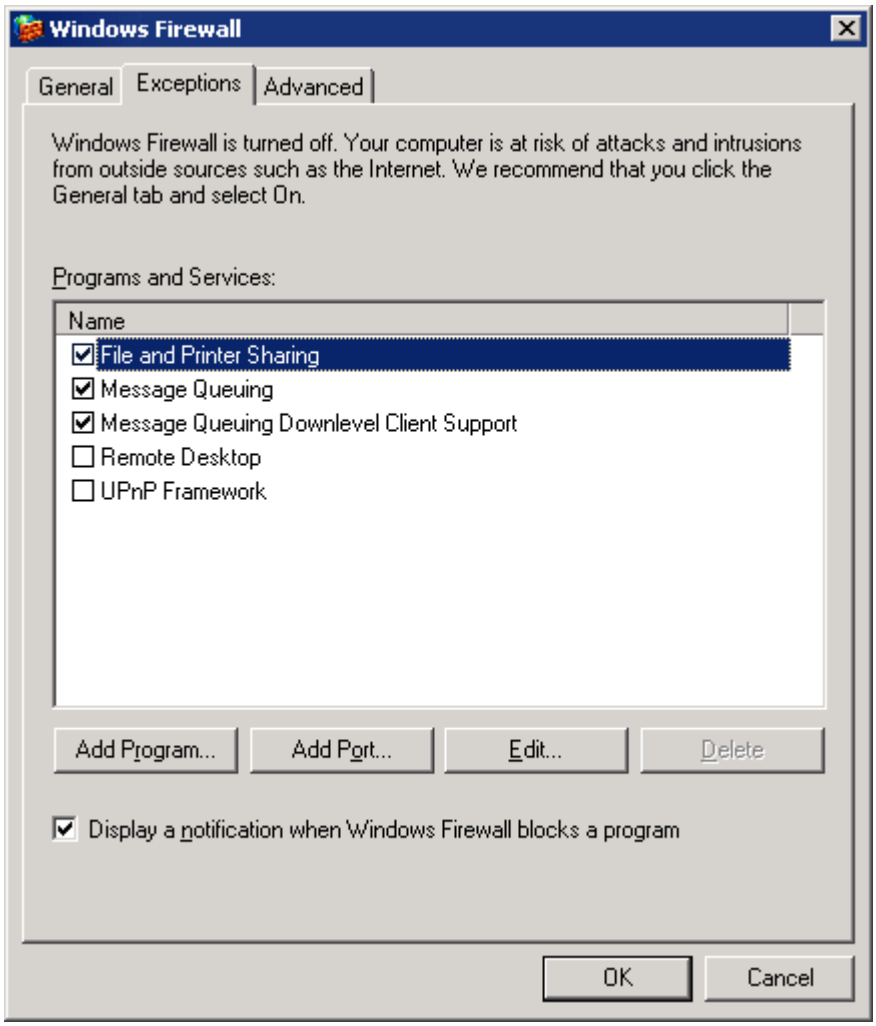
12. Close the **local Security Policy** window.

13.1.4 Microsoft Windows Server 2003

Enable Firewall permissions

To manually enable firewall rules on Microsoft Windows Server 2003:

1. Click **Start** ► **Control Panel** ► **Windows Firewall** and select **Exceptions** tab.



Screenshot 212 - Enable firewall rules in Microsoft Windows Server 2003

2. From **Programs and Services** list, enable **File and Printer Sharing**.

3. Click **OK** to apply changes and close.

13.1.5 Microsoft Windows Server 2008 (including R2)

Enable firewall permissions

To manually enable firewall rules on Microsoft Windows Server 2008 (including R2):

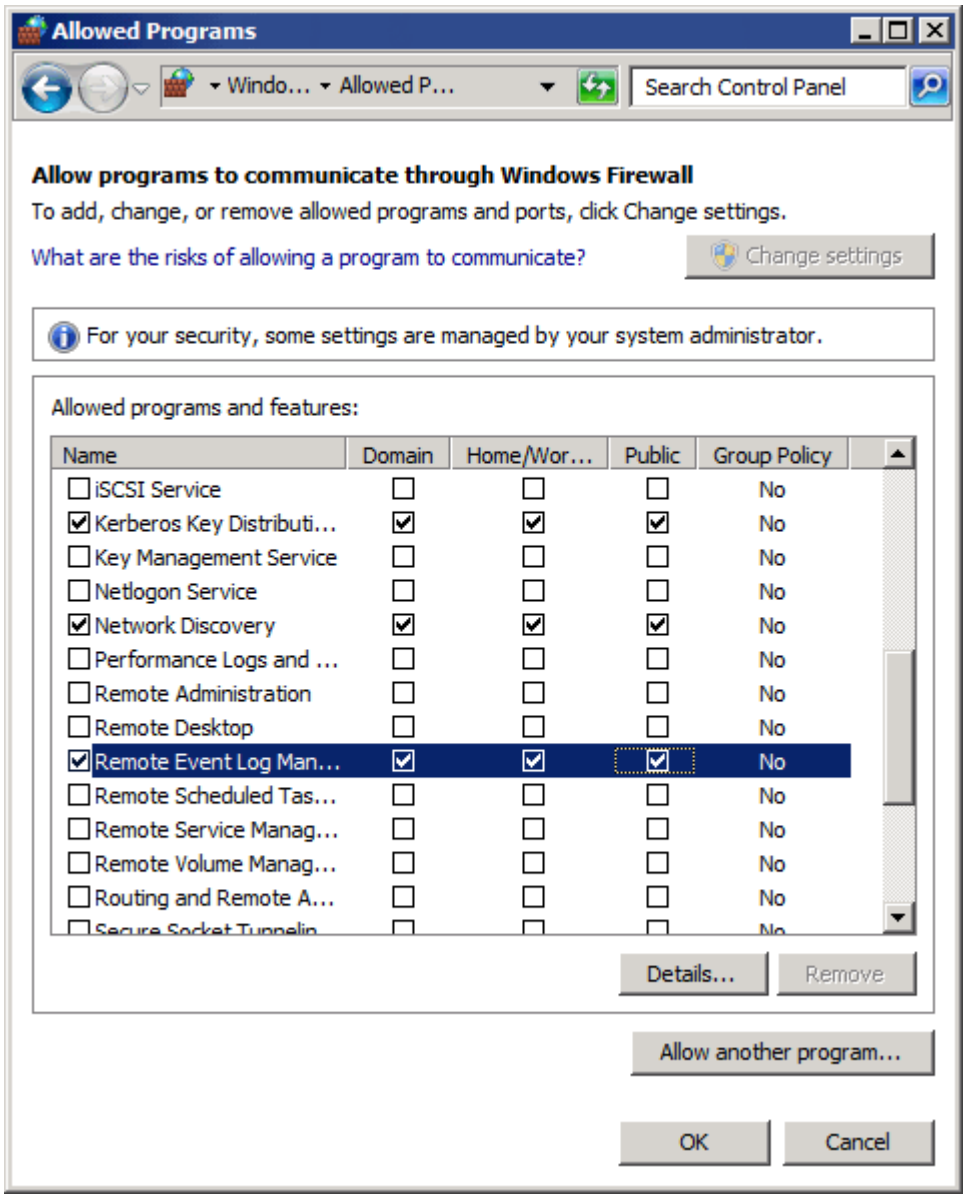
1. Click **Start** ► **Control Panel** ► **Security** and **Allow a program through Windows Firewall** under **Windows Firewall** category.

2. In the list of programs, enable the following:

» File and Printer Sharing

» Network Discovery

» Remote Event Log Management



Screenshot 213 - Firewall rules on Microsoft Windows Server 2008

3. Click **OK** to apply changes.

In Windows Server 2008 R2, ensure to select **Domain**, **Private** and **Public** for each rule mentioned above.

13.2 Setting permissions on target computers automatically via GPO

13.2.1 Windows Server 2003

To open ports and enable permissions on all domain clients using Microsoft Windows Server 2003 domain controller:

1. Click **Start** ► **Run**, key-in **mmc** and click **OK**.

2. Click **File** ► **Add/Remove Snap-in** and click **Add**.

3. Locate and select **Group Policy Object Editor** and click **Add**.

4. Click **Browse**, select **Default Domain Policy** and click **OK**.

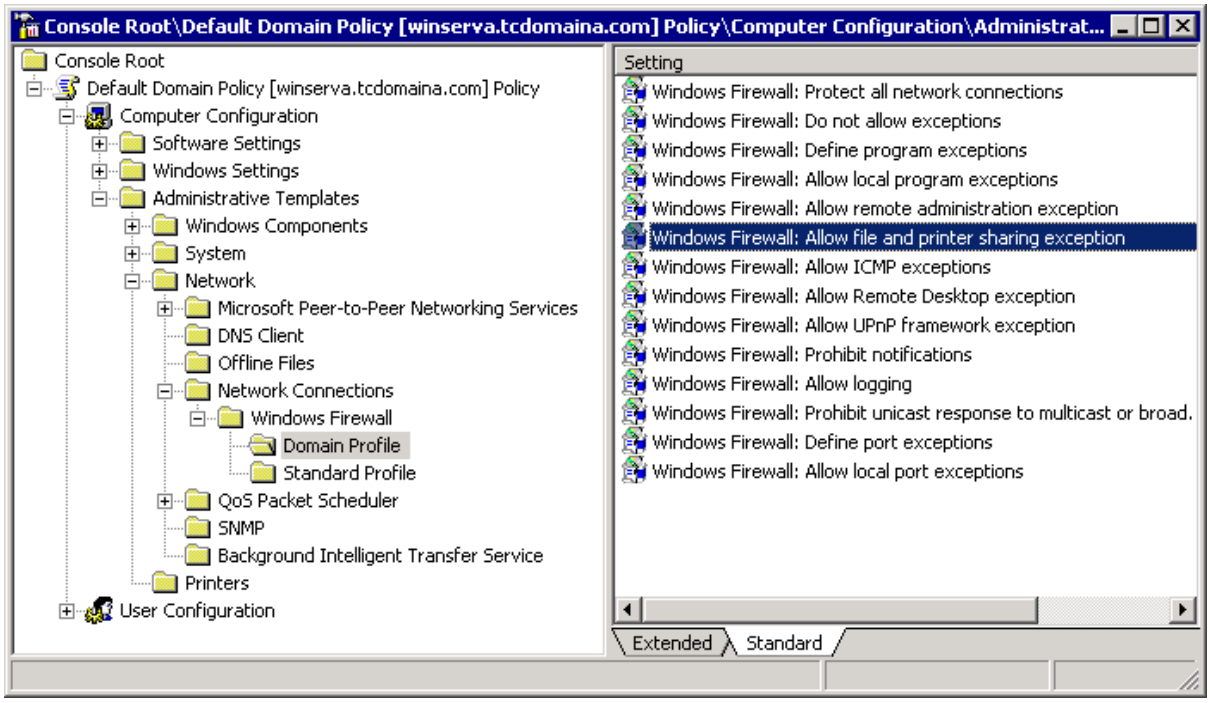
5. Click **Finish**.

6. Select **Group Policy Object Editor** again and click **Add**.

7. Click **Browse**, double click **Domain Controllers** folder and select **Default Domain Controllers Policy**. Click **OK**.

8. Click **Finish** and **Close**.

9. From the **Console Root**, expand **Default Domain Policy** ► **Administrative Templates** ► **Network** ► **Network Connections** ► **Windows Firewall** ► **Domain Profile**.



Screenshot 214 - Domain Policy console in Microsoft Windows Server 2003

10. From the **Settings** list, right click **Windows Firewall: Allow file and printer sharing exception** and select **Properties.**

11. From the **Settings** tab, select **Enabled** and click **OK**.

12. Repeat steps 9 to 11 for **Default Domain Controllers Policy**.

13. Click **File** ► **Save** to save the management console.

The group policy will be applied the next time each client machine is started.

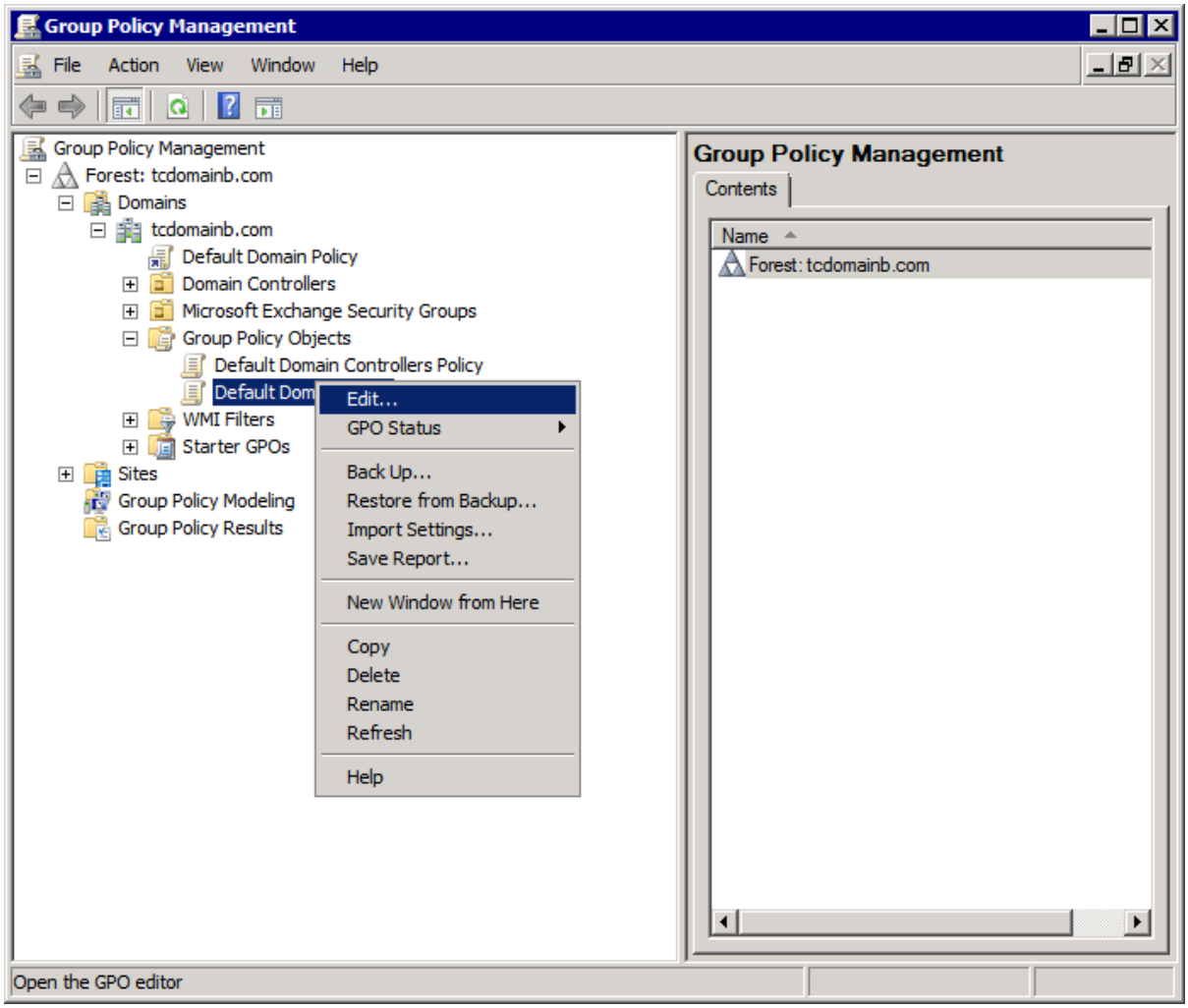
13.2.2 Windows Server 2008 (including R2)

Firewall permissions

To enable permissions on all domain clients:

1. Click **Start ► Administrative Tools ► Group Policy Management.**

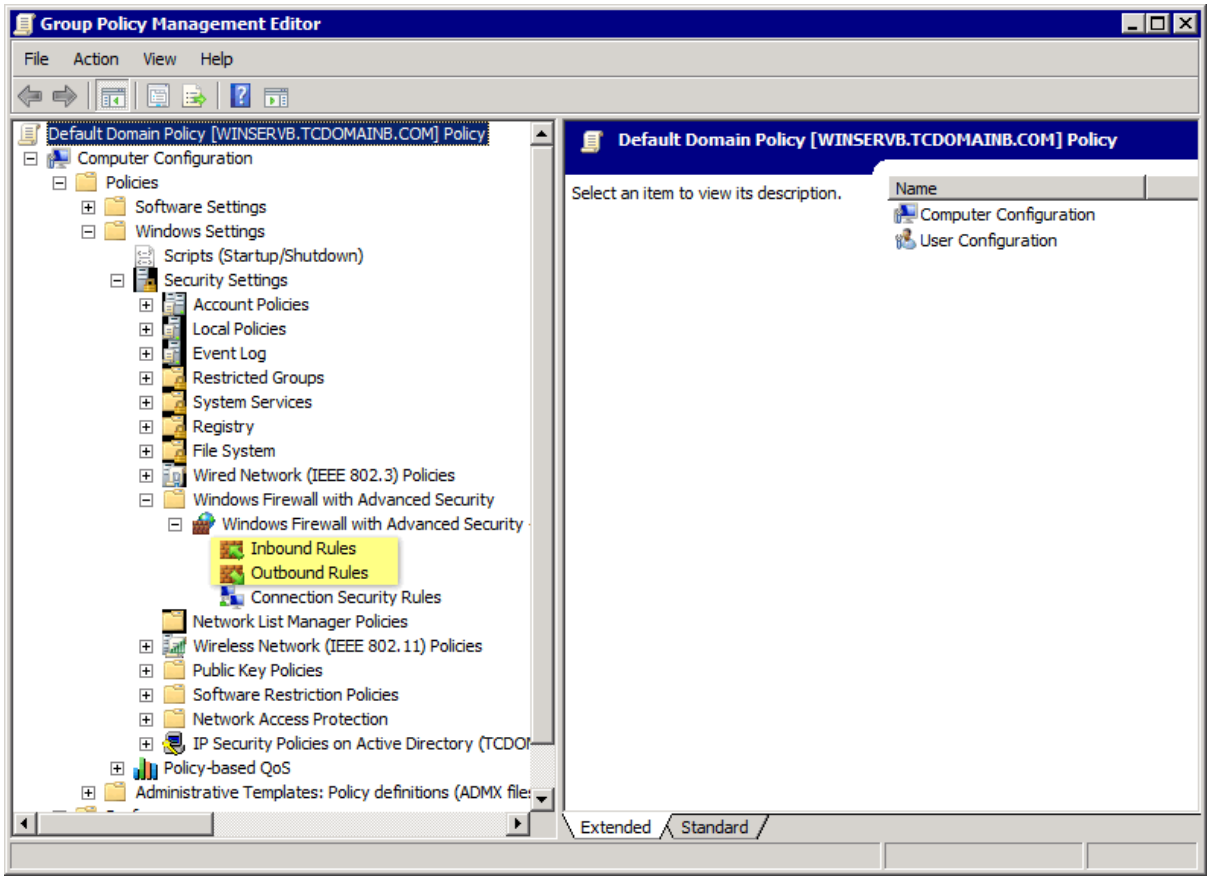
2. Expand **Group Policy Management ► Forest ► Domains ► <Domain name> ► Group Policy Objects.**



Screenshot 215 - Group Policy Management in Microsoft Windows Server 2008 R2

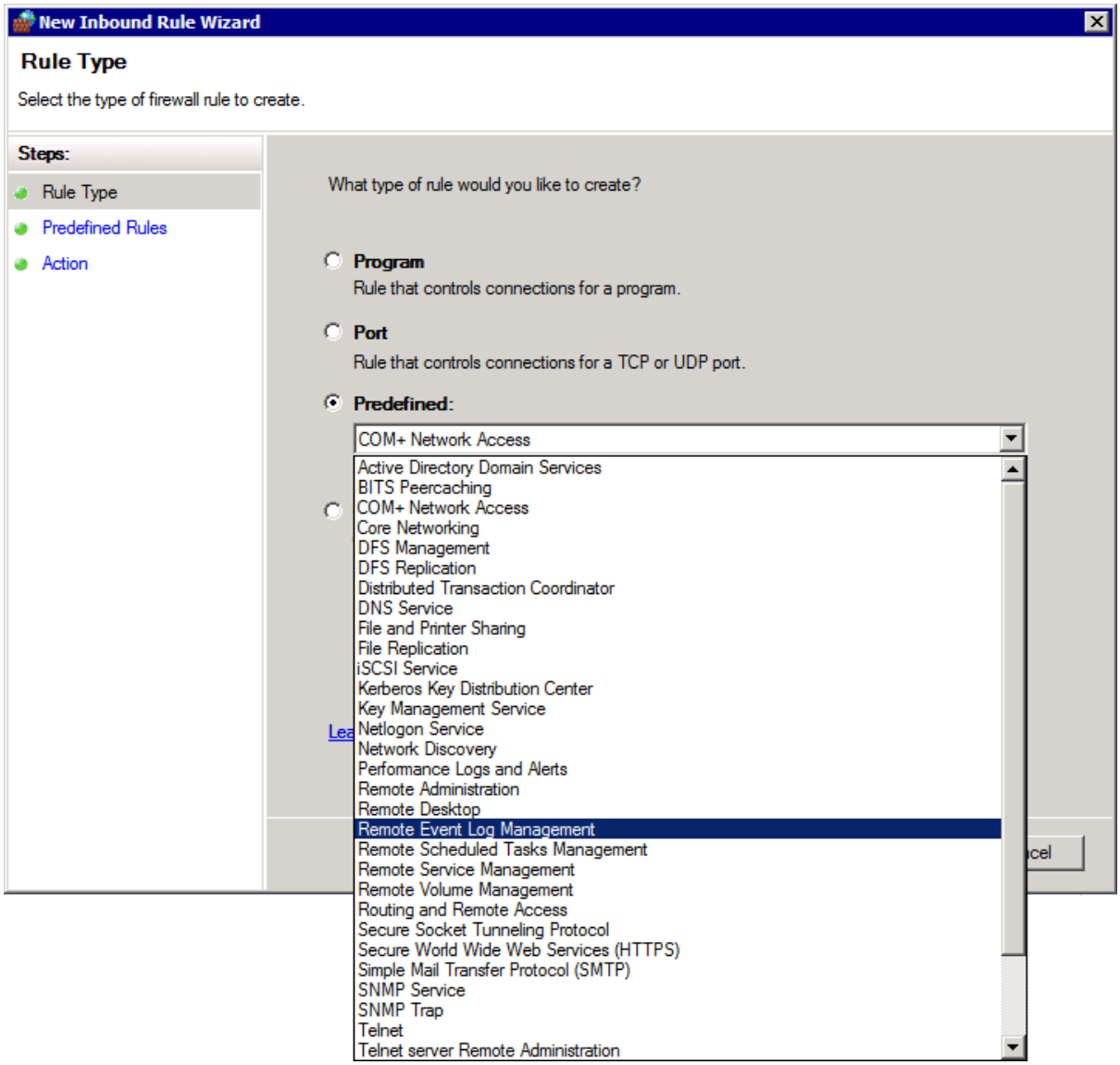
3. Right click **Default Domain Policy** and select **Edit.**

4. Expand **Computer Configuration ► Policies ► Windows Settings ► Security Settings ► Windows Firewall with Advanced Security**, right click **Inbound Rules** and select **New Rule…**



Screenshot 216 - Group Policy Management Editor

5. In the **New Inbound Rule Wizard**, select **Predefined** and select **File and Printer Sharing**.



Screenshot 217 - Predefined rules

6. Click **Next**.

7. Select all rules and click **Next**.

8. Select **Allow the connection** and click **Finish**

9. Repeat steps 5 to 8 for each of the following rules:

» Remote Event Log Management

» Network discovery

10. From Group Policy Management Editor, expand **Computer Configuration ► Policies ► Windows Settings ► Security Settings ► Windows Firewall with Advanced Security**, right click **Outbound Rules** and select **New Rule…**

11. Repeat Steps 5 to 9 while at step 9 enable only **Network Discovery**.

12. Close Group Policy Management Editor.

13. From Group Policy Management, expand **Group Policy Management ► Forest ► Domains ► <Domain name> ► Default Domain Controllers Policy.**

14. Repeat steps 4 to 13.

15. Close Group Policy Management.

The group policy will be applied the next time each client machine is started.

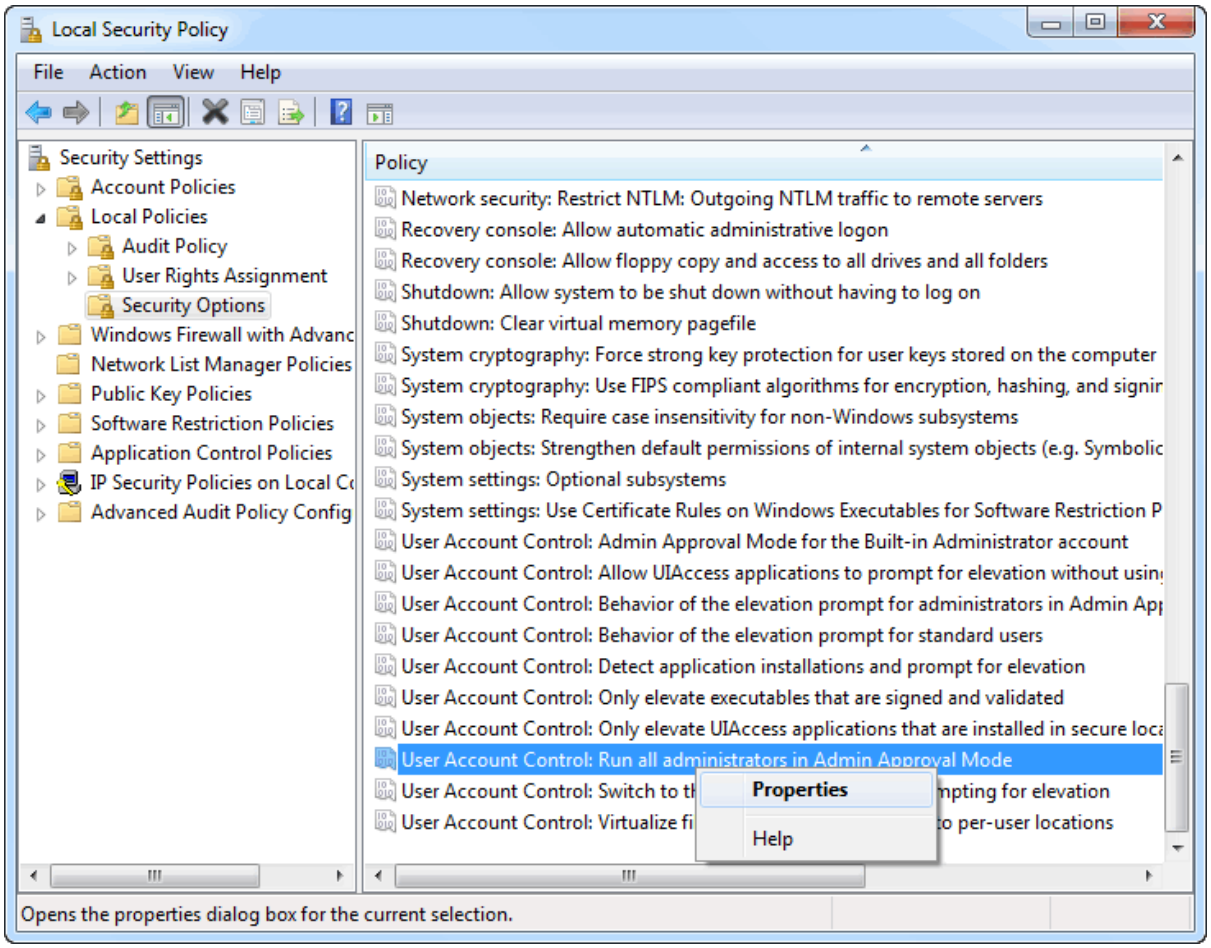
13.3 Disable UAC to scan target machines

When GFI EventsManager is configured to collect events using a local account target machines must have User Account Control (UAC) disabled. To disable UAC on Microsoft Windows Vista machines or later:

1. Click **Start ► Run**, key-in secpol.msc and press **Enter**.

2. From the **Security Settings**, expand **Local Policies** and click **Security Options**.

3. Right click **User Account Control: Run all administrators in Admin Approval Mode** and select **Properties**.


Local Security Policy
File Action View Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanc
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local C
Advanced Audit Policy Config
Policy
Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers
Recovery console: Allow automatic administrative logon
Recovery console: Allow floppy copy and access to all drives and all folders
Shutdown: Allow system to be shut down without having to log on
Shutdown: Clear virtual memory pagefile
System cryptography: Force strong key protection for user keys stored on the computer
System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signir
System objects: Require case insensitivity for non-Windows subsystems
System objects: Strengthen default permissions of internal system objects (e.g. Symbolic
System settings: Optional subsystems
System settings: Use Certificate Rules on Windows Executables for Software Restriction P
User Account Control: Admin Approval Mode for the Built-in Administrator account
User Account Control: Allow UIAccess applications to prompt for elevation without usin
User Account Control: Behavior of the elevation prompt for administrators in Admin Ap
User Account Control: Behavior of the elevation prompt for standard users
User Account Control: Detect application installations and prompt for elevation
User Account Control: Only elevate executables that are signed and validated
User Account Control: Only elevate UIAccess applications that are installed in secure loca
User Account Control: Run all administrators in Admin Approval Mode
User Account Control: Switch to th
User Account Control: Virtualize fi
Properties
Help
Opens the properties dialog box for the current selection.

Screenshot 218 - Predefined rules

4. From the **Local Security Settings** tab, select Enabled and click **OK**.

5. Close the **Local Security Policy** window.

13.4 Command line operations

GFI EventsManager provides you with three command line tools through which you can perform data export and import functions. These three tools are:

- **Exportdata.exe**: Exports data from an ESM 8 database using database operations engine
- **Importdata.exe**: Imports data into an EMS 8 database using database operations engine
- **Importsettings.exe**: Imports configuration from a data folder or from a configuration export file (.esmbkp) and is used mostly from installer when preserving configuration
- **ExportSettings.exe:** Exports configuration settings from GFI EventsManager installation to a configuration file.

- **ExportRules.exe:** Creates an HTML document that contains details on the processing rules configured in a GFI EventsManager installation.
- **Esmreport.exe:** Generates in-product reports such as configuration and job activity reports.

13.4.1 Exportdata.exe

Use this tool to export data from the GFI EventsManager database to binary file.

exportdata.exe <parameters list>

PARAMETER	MANDATORY/OPTIONAL	DESCRIPTION
/folder: <path & foldername>	Mandatory	Defines folder where the data file will be stored. **IMPORTANT:** The folder must be created before executing the command.
/period: <number of hours>	Optional	Exports events older than the number of hours: Default = 7 days
/password: <file password>	Optional	Sets an encryption password
/delete	Optional	Deletes the events after export
/movetodb:<database name>	Optional	Moves the events to another database on the same server. If no name is specified, the backup database will be used

Any parameter that contains spaces must be enclosed in double quotes (“).

Example:

Exportdata.exe /folder:c:\exportfiles /period:240 /password:aip112sK

Data exported using the above command:

- A folder called **exportfiles**, located at **c:**
- Data older than 10 days (**240hours**)
- Encrypt using password **aip112sK**

13.4.2 Importdata.exe

Use this tool to import data in binary files to the GFI EventsManager database.

importdata.exe <parameters list>

PARAMETER	MANDATORY/ OPTIONAL	DESCRIPTION
/folder:<path & foldername>	Mandatory	Defines the folder where the data file is stored.
/password:<file password>	Optional	Defines the password that will be used to decode files; if not specified, no password will be used
/dbserver:<databaseserver location >	Optional	Defines the database server where the destination database lies. If not specified, the database details specified in GFI EventsManager will be used.
/dbname:<database name>	Optional	Defines the destination database name. If not specified, the database name specified in GFI EventsManager will be used.
/dbuser:<username>	Optional	Defines the user name used to connect to database. If not specified, Windows authentication will be used.

PARAMETER	MANDATORY/ OPTIONAL	DESCRIPTION
/dbpass:<password>	Optional	Defines the password used to connect to destination server/database. If none is specified, password is ignored.

Any parameter that contains spaces must be enclosed within double quotes (“).

Example:

importdata.exe /folder:c:\exportfiles /password:aip112sK /dbserver:192.168.3.55 /dbname:mainesmdb /dbuser:sa /dbpass:sapwd

Data exported using the above command:

- From folder called **exportfiles**, located at **c:**\
- Decrypted using password **aip112sK**
- Saved to database on server with **IP address 192.168.3.55**, **with database name: mainesmdb** and with the following **login credentials: username: sa** and **password sapwd**.

13.4.3 ImportSettings.exe

Use this tool to import GFI EventsManager configurations previously exported.

importsettings.exe <parameters list>

PARAMETER	MANDATORY/OPTIONAL	DESCRIPTION
/operation:<operation>	Mandatory	Defines the operation to perform, either importfolder or importfile
/destination:<destination path>	Optional	Defines the destination folder where the configuration will be imported
/sourceFile:<filename>	Optional	Defines the name of the file that contains the exported GFI EventsManager configuration.
/sourceFolder:<folder name/path>	Optional	Defines the name of the folder that contains the exported GFI EventsManager configuration.

Any parameter that contains spaces must be enclosed in double quotes (“).

Example:

importsettings.exe /operation:importfolder: /destination: c:\esm\data /sourcefolder: c:\esm\old

Where data is imported with the following details:

- Operation is importfolder to c:\esm\data from folder c:\esm\old

13.4.4 ExportSettings.exe

Use this tool to export the GFI EventsManager configuration.

exportsettings.exe <parameters list>

PARAMETER	MANDATORY/OPTIONAL	DESCRIPTION
/destination:<filename>	Mandatory	Defines the file where the configuration will be exported
/folder:<folder>	Optional	To export from an alternative folder.

Any parameter that contains spaces must be enclosed in double quotes (“).

Example:

exportsettings.exe /destination:”c:\export”

Where data is exported with the following details:

» Export file located in C:\export.esmbkp

13.4.5 ExportRules.exe

Use this tool to create an HTML document containing all processing rules.

The HTML document is exported to:

» **<GFI EventsManager home Directory> \ Configuration Reports \ Reports <current date>**

Example:

C:\Program Files\GFI\EventsManager 8\Configuration reports\Reports 2010-02-23\

» Select a computer from the HTML document to display all processing rules related to the computer selected.

» Select a processing rule from the HTML document to display the conditions that apply to the rule selected.

For more information, refer to http://kbase.gfi.com/showarticle.asp?id=KBID003785.

13.4.6 Esmreport.exe

Use this tool to generate **Configuration** and **Status** reports.

esmreport.exe <general parameters list>

PARAMETER	TYPE	DESCRIPTION
/format:<*format*>	HTML/CSV	Define the format of the resulting report.
/type:<*type*>	Configuration/Status	Define the type of report to generate.

esmreport.exe <additional parameters list for Configuration reports>

PARAMETER	DESCRIPTION
/source:<*name*>	Specify the name of the event source to report on. **NOTE**: Source names with spaces must be quoted. Example: » /source:”My event source”
/group:<*name*>	Specify the name of the event source group to report on. **NOTE**: Source group names with spaces must be quoted. Example: **/source:”My event source group”**

esmreport.exe <additional parameters list for Status reports>

PARAMETER	DESCRIPTION
/subtype:<*subtype*>	The subtype parameter can have the following values: » **Messages** - reports on messages from Job Activity ► Operational history » **Stats** - generates the report based on data from Statistics ► Activity overview

PARAMETER	DESCRIPTION
/period:<*period*>	Period parameter can have the following values: » **all time** - generates report based on all stats displayed in the panel. Valid only for **stats** subtype. » **current** - generates report based on all messages displayed. Valid only for **messages** subtype » A specific date - will export stats/messages of the specified date. **NOTE**: Periods with spaces must be quoted. Example: » /period:"all time"
/options:<*option1*>,<*option2*>	Optional parameters can have the following values: **error messages** - will generate the report for error messages. Valid only for **stats** subtype **only with issues** - generates the report based on event sources with scanning issues (not scanned). **NOTE**: Options with spaces must be quoted. Example: » /options:"error messages" » **/options:"only with issues"**

Example:

» esmreport.exe /type:configuration /target:"C:\My reports\EventsManager /format:HTML

» esmreport.exe /type:status /subtype:messages /period:"all time" /options:"error messages"

13.4.7 Customizing unique identifiers

GFI EventsManager enables you to customize the unique identifiers of the GFI EventsManager installation. This enables you to import the same configuration into separate without incurring duplicate GFI EventsManager instance IDs.

To configure new GFI EventsManager unique identifiers add the following option to command line options of importdata.exe

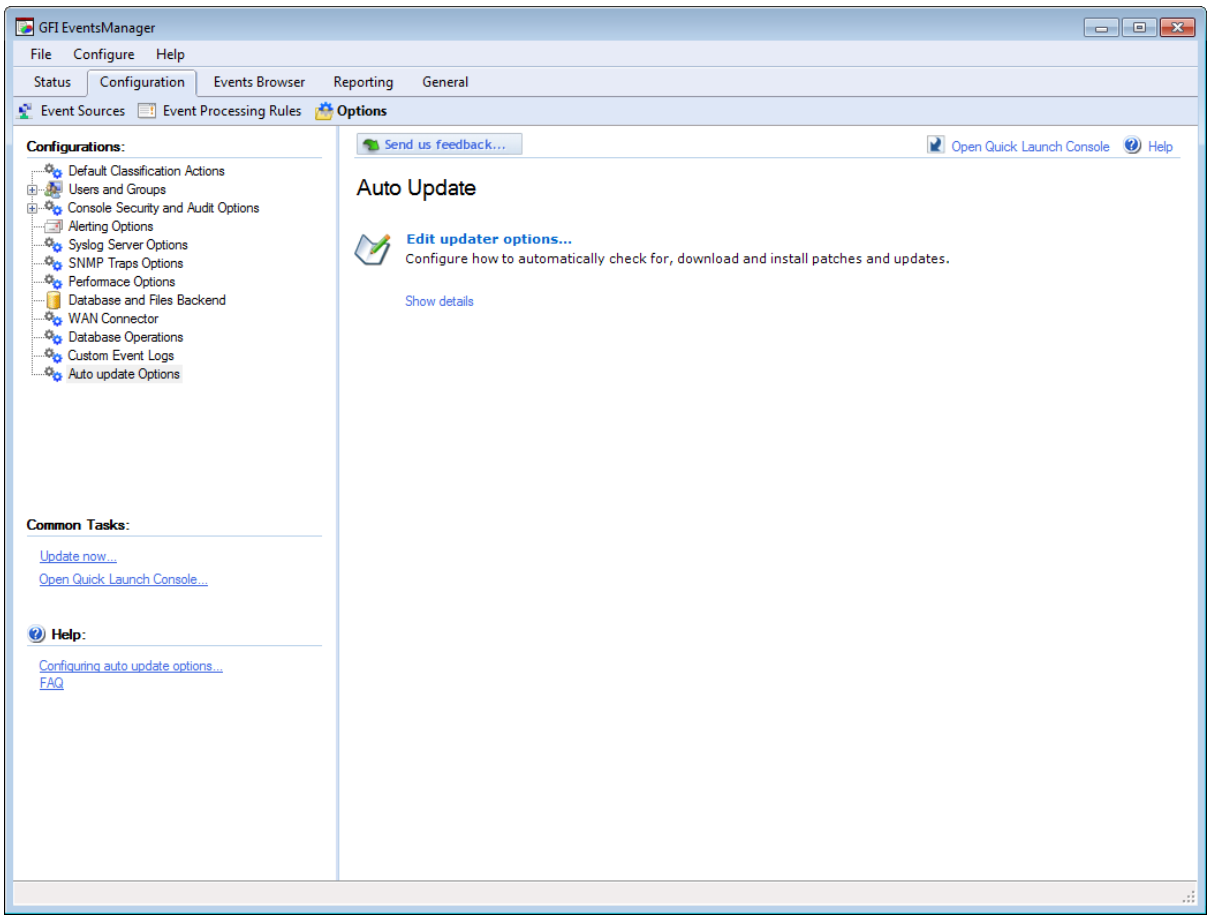
PARAMETER	MANDATORY/OPTIONAL	DESCRIPTION
/id:<new_id>	Optional	Defines the new ESM instance id set after importing the configuration. Use this parameter on only if you only want to change the ESM instance id; if no value is specified the existing ESM instance id will be preserved.

13.5 Auto updating GFI EventsManager

GFI EventsManager enables users to configure how to automatically check for, download and install patches and updates.

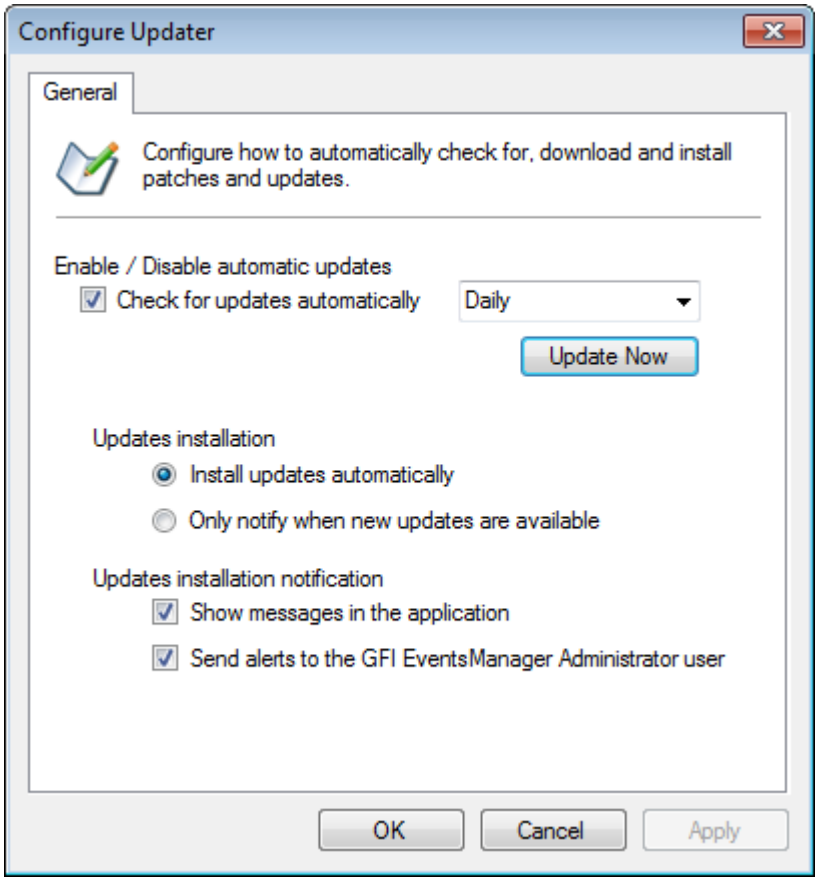
To configure Auto Update options:

1. Launch GFI EventsManager from **Start ►Program ►GFI EventsManager ► Management Console.**



Screenshot 219 - Auto update options

2. Click **Edit updater options…**



Screenshot 220 - Configure auto update

3. Configure the options described in Table 33 below and click **OK**:

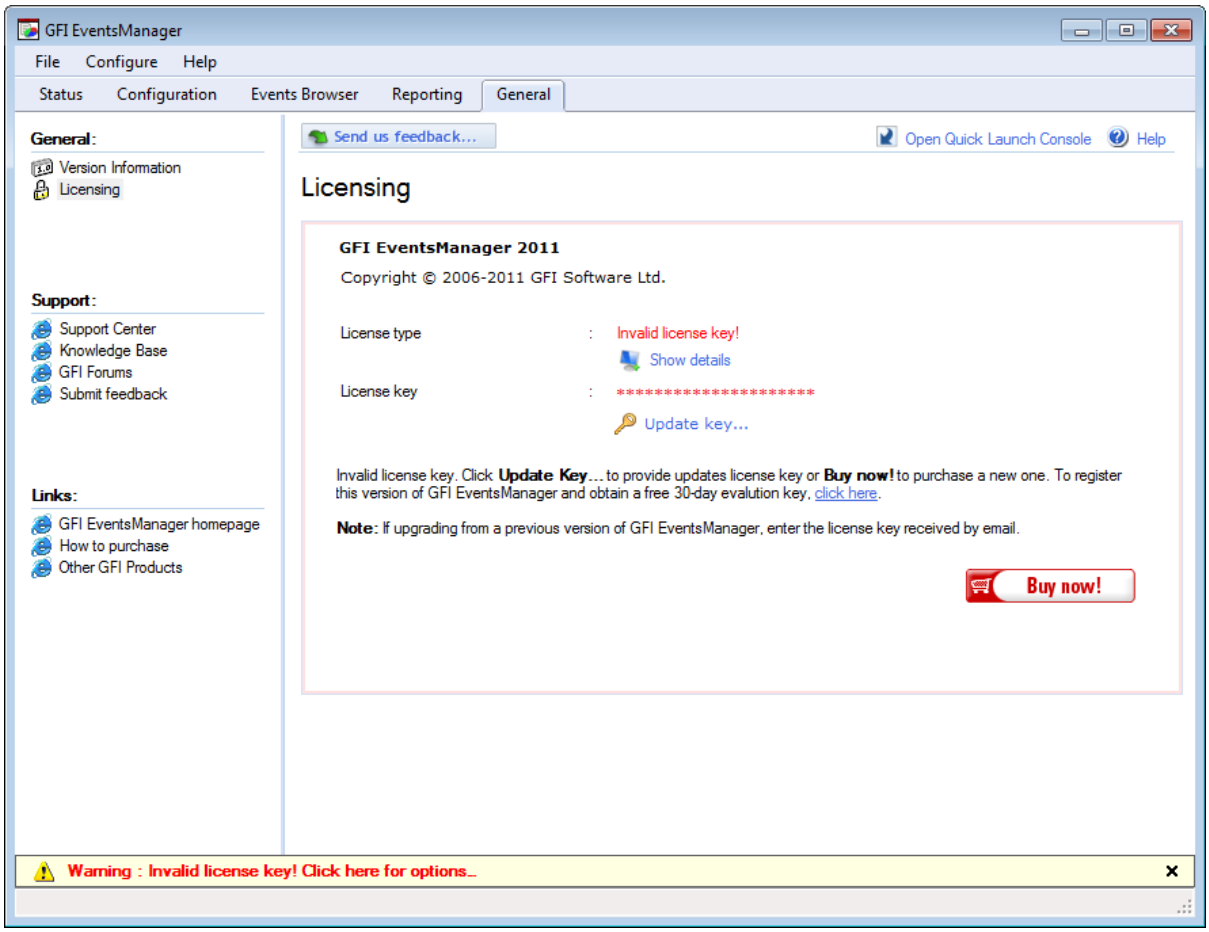
Table 33 - Auto update options

OPTION	DESCRIPTION
Check for updates automatically	If selected, GFI EventsManager will check for updates automatically on a daily or weekly basis.
Update Now	If **Check for updates automatically** checkbox is not selected, use this option to manually check for updates and install missing updates.
Install updates automatically	Installs downloaded updates automatically.
Only notify me when updates are available	Available updates are shown in the **Missing Updates** section but are not installed.
Show messages in the application	Shows a message at the bottom of the application page. Click on the displayed message to action the updates.
Send alerts on GFI EventsManager Administrator user	Sends an email alert on the configured GFI EventsManager Administrator account. For information on configuring GFI EventsManager Administrator account refer to Configuring the Administrator account section in this manual.

13.6 Product licensing

GFI EventsManager is licensed by Node. All devices that generate a log are considered to be a Node.

Licensing Page

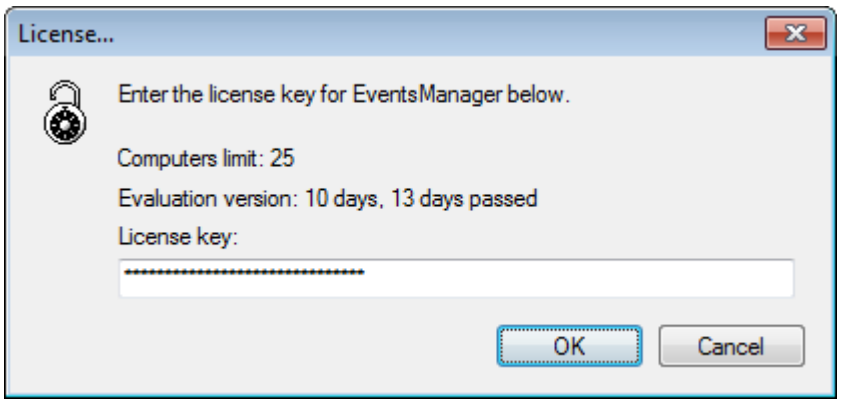

GFI EventsManager
File Configure Help
Status Configuration Events Browser Reporting General
General:
Version Information
Licensing
Support:
Support Center
Knowledge Base
GFI Forums
Submit feedback
Links:
GFI EventsManager homepage
How to purchase
Other GFI Products
Send us feedback...
Open Quick Launch Console
Help
Licensing
GFI EventsManager 2011
Copyright © 2006-2011 GFI Software Ltd.
License type : Invalid license key!
Show details
License key : **********
Update key...
Invalid license key. Click Update Key... to provide updates license key or Buy now! to purchase a new one. To register this version of GFI EventsManager and obtain a free 30-day evalution key, click here.
Note: If upgrading from a previous version of GFI EventsManager, enter the license key received by email.
Buy now!
Warning : Invalid license key! Click here for options...

Screenshot 221 - Licensing page

13.6.1 To update license key

1. Click **General** tab.

2. From the left pane, right-click **Licensing**, select **Update license key...**.



Screenshot 222 - Update license key

3. Specify your license key details.

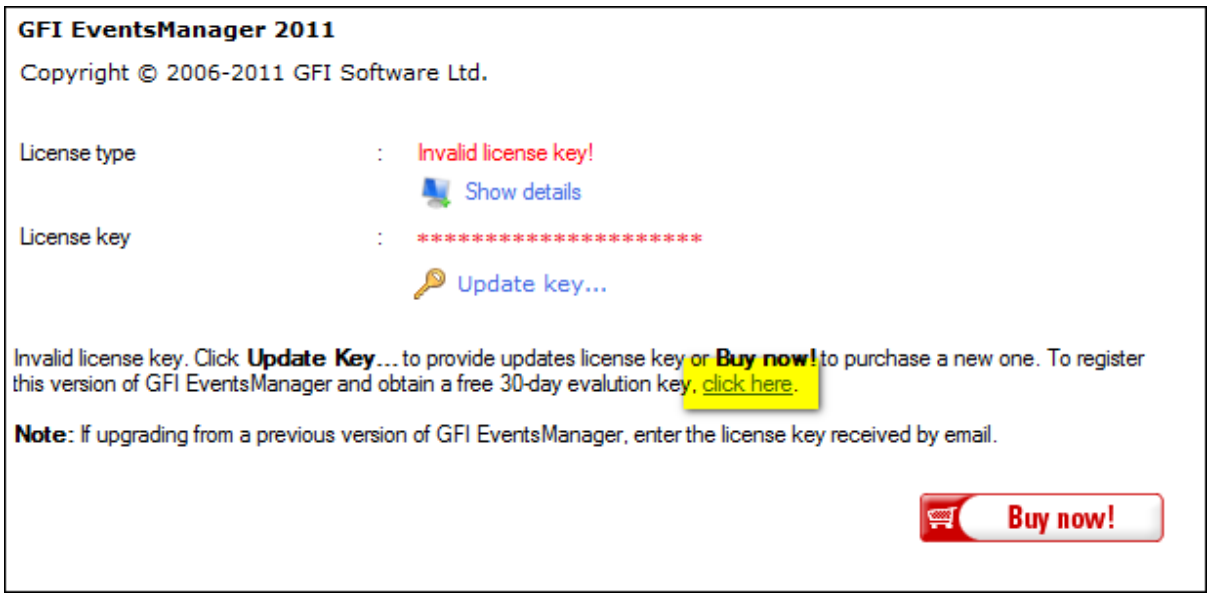
4. Click **OK** to finalize settings.

13.6.2 To obtain a free 30-day trial license key

GFI EventsManager allows you to register your version of the product and receive a free 30-day trial. Once the trial period is expired, all event log monitoring and management services are disabled and a full license key is required.

To register and receive a 30-day trial license key:

1. Click **General** tab.


GFI EventsManager 2011
Copyright © 2006-2011 GFI Software Ltd.
License type : Invalid license key!
Show details
License key : **********
Update key...
Invalid license key. Click Update Key... to provide updates license key or Buy now! to purchase a new one. To register this version of GFI EventsManager and obtain a free 30-day evalution key, click here.
Note: If upgrading from a previous version of GFI EventsManager, enter the license key received by email.
Buy now!

Screenshot 223 - Register link

2. Click the provided link. This will take you to GFI website where you are able to enter you details and receive the license key by email.

The email address you provide in the registration form is where your free 30-day trial key will be sent. If you have a spam filtering system, make sure the email is not blocked as spam.

13.6.3 To view license details

1. Click **General** tab.

2. From the left pane, click **Licensing** option. Licensing details will be displayed in the right pane of the management console.

3. To view license distribution details click on **Show Details**. This will show the number of event sources configured and respective license type (such as Workstation or Server).

13.6.4 To update license type

To change the type of license allocated to a specific event source:

1. Launch the (computer/computer group) properties dialog and click the **Licensing Type** tab.

2. By default event sources inherit their licensing type from parent group (use the license type configured in parent group properties). To change license type select the Server License or Workstation option accordingly.

13.6.5 To purchase a license key

1. Click **General** tab.

Screenshot 224 - Buy now! button

2. From the right pane, click **Buy now!**. This takes you to GFI website where you can view further information about licensing and purchase a valid key.

For more information about GFI EventsManager licensing, please visit: http://www.gfi.com/page/13789/products/gfi-eventsmanager/pricing/licensing/licensing

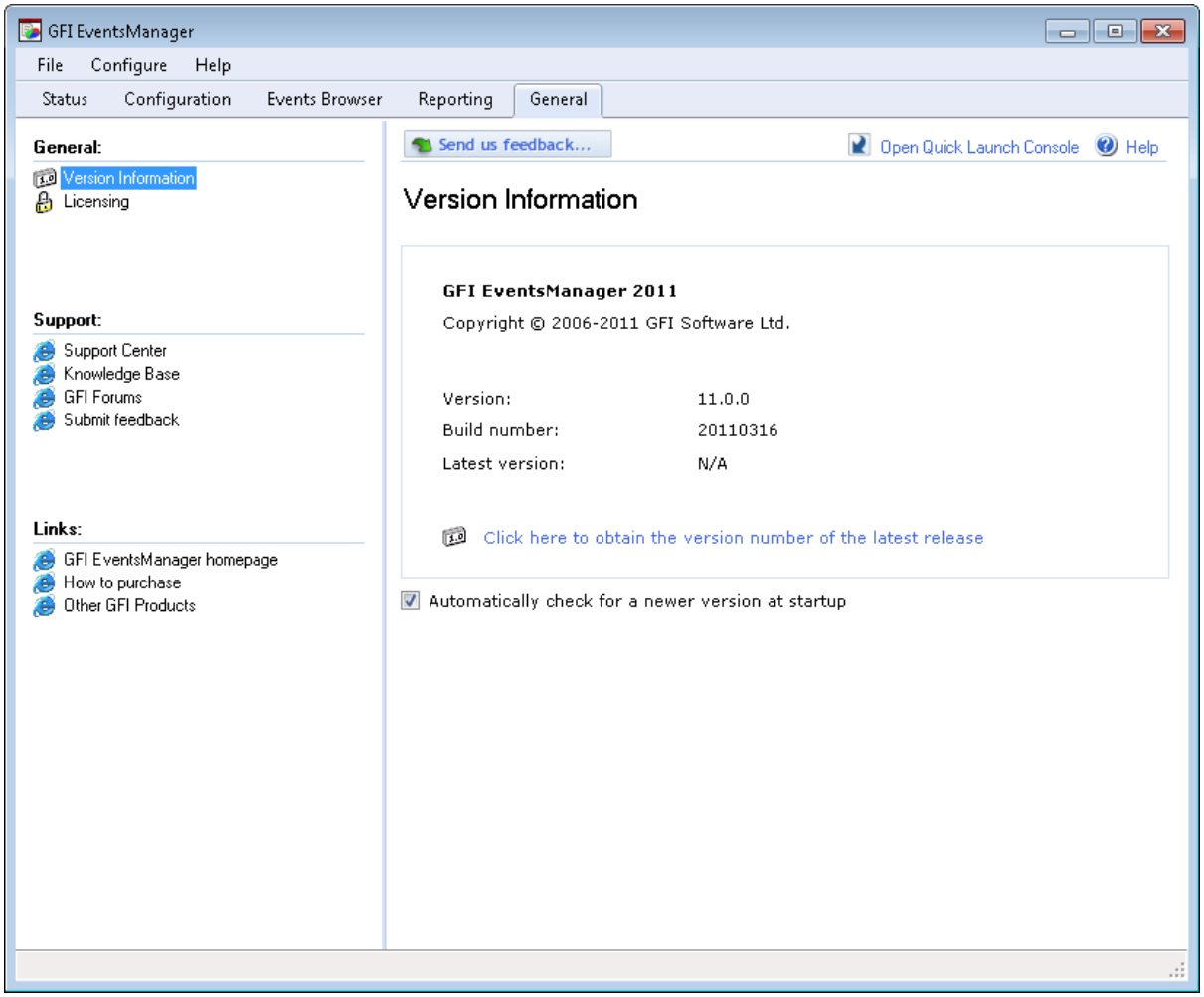
For more information about GFI EventsManager pricing, please visit: http://www.gfi.com/products/gfi-eventsmanager/pricing

13.7 Version information

To check your version information details:

1. Click **General** tab.

2. Click the **Version Information** option. The version information details will be displayed in the right pane.



Screenshot 225 - Version Information screen

13.7.1 Checking for newer builds

To check for newer builds of GFI EventsManager:

1. Click **General** tab.

2. From the left pane, right-click **Version Information** and select **Check for newer builds**….

14 Troubleshooting

14.1 Introduction

The troubleshooting chapter explains how you should go about resolving any software issues that you might encounter. The main sources of information available to users are:

- The manual - most issues can be solved by reading this manual
- GFI Knowledge Base articles
- Web forum
- Contacting the GFI Technical Support

14.2 Common issues

ISSUE	DESCRIPTION AND SOLUTION
Error message: Not connected to the database or connection was lost.	**Description** This error is encountered when GFI EventsManager is unable to connect with the SQL Database or the database connection was interrupted. **Solution** The following links contain information on how this issue can be solved. How do I debug 'Failed to connect to database'? http://kbase.gfi.com/showarticle.asp?id=KBID002855 How do I configure SQL Server 2005/2008 to accept SQL Authentication? http://kbase.gfi.com/showarticle.asp?id=KBID002804 How do I configure SQL Server 2000 to accept SQL Authentication? http://kbase.gfi.com/showarticle.asp?id=KBID002805 Enabling TCP/IP on Microsoft SQL Server 2005 http://kbase.gfi.com/showarticle.asp?id=KBID002920 How to create a new database in Microsoft SQL Server http://kbase.gfi.com/showarticle.asp?id=KBID003379
Error message: Primary Filegroup Full.	**Description** This error is encountered when GFI EventsManager database backend has a maximum file size limitation and is unable to store any further data. **Solution** Configure the database backend to allow larger file size. This can be done on both Microsoft SQL Server and Microsoft SQL Server Express edition. For more information on how to change the maximum file size, refer to http://kbase.gfi.com/showarticle.asp?id=KBID003670
Error message: Could not complete cursor operation because the table schema changed after the cursor was declared'	**Description** This error is encountered when the administrator is performing maintenance tasks on the GFI EventsManager databases while the GFI EventsManager service is running. **Solution** 1. Stop GFI EventsManager service 2. Perform the maintenance tasks in Microsoft SQL server 3. Restart GFI EventsManager Service once the Microsoft SQL maintenance tasks are finished. To avoid this, ensure that GFI EventsManager service is stopped whilst performing any maintenance tasks on the GFI EventsManager database. For more information refer to http://kbase.gfi.com/showarticle.asp?id=KBID003011

ISSUE	DESCRIPTION AND SOLUTION
Error message 1: Error connecting to machine MACHINENAME, Error 0x35, Message: The network path was not found. **Error message 2:** Error connecting to machine MACHINENAME, Error 0x52E, Message: Logon failure: unknown user name or bad password. **Error message 3:** Critical error encountered: A network-related or instance-specific error occurred while establishing a connection to SQL Server. The server was not found or was not accessible. Verify that the instance name is correct and that SQL Server is configured to allow remote connections. (provider: Named Pipes Provider, error: 40 - Could not open a connection to SQL Server) **Error message 4:** Unexpected error when connecting to machine MACHINENAME; remote W3C logs path is: PATH*.*	**Description** These errors are encountered when GFI EventsManager tries to collect events from a machine that is not accessible over the network or the credentials are invalid. **Possible solution 1** 1. Check that the credentials are correct 2. Check that the machine name or IP address are correct 3. Try to collect events **Possible solution 2** When using a personal firewall, check that the required firewall ports are configured to allow traffic. For more information refer to http://kbase.gfi.com/showarticle.asp?id=KBID002770 When using Windows firewall, check that all the required firewall permissions are enabled. For more information refer to http://kbase.gfi.com/showarticle.asp?id=KBID003688 **Possible solution 3** Ensure that GFI EventsManager is installed on a supported environment. For more information on where GFI EventsManager can be installed, refer to http://kbase.gfi.com/showarticle.asp?id=KBID002842
No event logs are being collected by GFI EventsManager.	**Description** This issue can be caused by various factors and is dependent on the environment where GFI EventsManager is installed. For a checklist on how to resolve this issue, refer to http://kbase.gfi.com/showarticle.asp?id=KBID002819

ISSUE	DESCRIPTION AND SOLUTION
Error message 1: A timeout was reached (60000 milliseconds) while waiting for the GFI EventsManager service to connect. **Error message 2:** Error 1053: The service did not respond to the start or control request in a timely fashion.	**Description** The GFI EventsManager executables are digitally signed by default. When trying to start the service, the application must download the Certificate Revocation List to authenticate. If the download fails due to network connectivity or security reasons the service will fail to start by timing out. **Possible solution 1** Increase the default service timeout settings as described in the following Microsoft knowledgebase article http://support.microsoft.com/kb/941990 **Possible solution 2** Disable Certificate revocation list (CRL). 1. Download Microsoft Setreg application from http://ftp.gfisoftware.com/support/setreg.zip 2. Login to the GFI EventsManager server using the GFI EventsManager service user. 3. Open command prompt 4. Change the directory to the directory storing setreg.exe 5. Run the following command: setreg.exe 3 FALSE **Note:** The setting above can be reverted by running the following command: setreg.exe 3 TRUE For more information refer to http://kbase.gfi.com/showarticle.asp?id=KBID003365
Error message: The maintenance job failed!	**Description** GFI EventsManager uses an ASP.Net Library called GZipStream to compress and export data from the GFI EventsManager databases. GZipStream is unable to compress data larger than 4GB. GFI EventsManager will return this error when trying to export data which is larger than 4GB. **Solution** In order to export the data required, use the GFI EventsManager Advanced Filters to reduce the number of Events exported. Therefore eventually reducing the size of the data which is being compressed. For more information, refer to Configuring data filter conditions section in this manual.
Error message: Event Log Records could NOT be retrieved: The RPC server is unavailable	**Description** This error may occur if: » The remote computer may be shut down. » There may be a network hardware problem. » There may be no common transports. » The remote computer does not exist. » A DNS entry does not exist for the remote computer in the DNS server (Try pinging the remote machine from another computer by using its host name and not its IP). Investigate each possible problem and make the necessary changes. Then try to collect events from target computers. For more information, refer to http://kbase.gfi.com/showarticle.asp?id=KBID002820

ISSUE	DESCRIPTION AND SOLUTION
GFI EventsManager reports an error number 1069.	**Description** When installed, GFI EventsMananger asks for a valid username and password. This error is encountered when an invalid password is submitted in the installation wizard. **Solution** 1.Click **Start** ► **Run,** key-in services.msc and click **Ok**. This will launch **Services** window. 2. Double Click **GFI EventsManager** service. 3. Select the **Log On** tab. 4. Ensure that the **This account** radio box is selected. 5. Key-in a valid password for the specified User account. 6. Press **OK** to close the Properties window. 7. Close **Services** window.
When collecting and processing events the CPU consumption stays constant and higher than 70%.	**Description** This may occur when scanning multiple domain controllers. Since domain controllers generate a large number of events and GFI EventsManager by default is configured to use a high performance level, GFI EventsManager may use a lot of CPU resources. **Solution** Configure GFI EventsManager to use a low performance level. To configure performance level: 1. Select **Configuration** tab. 2. From the left panel, right click **Performance Options** and select **Edit Performance options**. 3. From the **Performance Options** dialog, select **Enable GFI EventsManager service performance** and select the required level. 4. Click **OK**. Changing the performance level reduces CPU load but affect GFI EventsManager log events processing speed. **Low performance** - GFI EventsManager will Approximately process 50 events per second for each event source. **High performance** - GFI EventsManager will Approximately process from 1000 to 2000 events per second for event source.

14.3 Knowledge Base

GFI maintains a Knowledge Base, which includes answers to the most common problems. If you have a problem, please consult the Knowledge Base first. The Knowledge Base always has the most up-to-date listing of technical support questions and patches. To access the Knowledge Base, visit http://kbase.gfi.com/.

14.4 Web Forum

User to user technical support is available via the web forum. The forum can be found at: http://forums.gfi.com/.

14.5 Request technical support

If you have referred to this manual and our Knowledge Base articles, and you still cannot solve issues with the software, contact the GFI Technical Support team by filling in an online support request form or by phone.

- **Online:** Fill out the support request form on: http://support.gfi.com/supportrequestform.asp. Follow the instructions on this page closely to submit your support request.
- **Phone:** To obtain the correct technical support phone number for your region please visit: http://www.gfi.com/company/contact.htm.

Before you contact our Technical Support team, please have your Customer ID available. Your Customer ID is the online account number that is assigned to you when you first register your license keys in our Customer Area at: http://customers.gfi.com.

We will answer your query within 24 hours or less, depending on your time zone.

14.6 Build notifications

We strongly suggest that you subscribe to our build notifications list. This way, you will be immediately notified about new product builds. To subscribe to our build notifications, visit:

http://www.gfi.com/pages/productmailing.htm.

15 Glossary

Table 34 below describes all common terms used in this manual:

Table 34 - Terms used in this manual

TERM	DEFINITION
Audit process tracking	Generates events which track actions such as programs which are launched, closed, as well as other indirect object access information which contain important security information. For more information, refer to http://technet.microsoft.com/en-us/library/cc775520(WS.10).aspx
Actions	The activity that will be carried out as a result to events matching specific conditions. For example you can trigger actions whenever an event is classified as critical. Actions supported by GFI EventsManager include Email alerts, event archiving and execution of scripts.
Alerts	Notifications which inform recipients that a particular event has occurred. GFI EventsManager can generate Email alerts, SMS alerts and Network alerts.
Archive	A collection of events stored in the SQL Server based database backed of GFI EventsManager.
Audit account management	Generates events when account management operations are done such as create/delete a user account or group, enable/disable a user account and set/change a user password. For more information, refer to http://technet.microsoft.com/en-us/library/cc737542(WS.10).aspx
Audit system events	Generates events when important system events happen such as user restarts or shuts down the target computer or when an event occurs that affects the security log. For more information, refer to http://technet.microsoft.com/en-us/library/cc782518(WS.10).aspx
COM+ Network Access	Enable this firewall permission to allow client machines to access applications or services that resides on the server. This allows GFI EventsManager to access resource from all servers. For more information about this permission, refer to http://technet.microsoft.com/en-us/library/cc731967.aspx
Email alerts	Email notifications which inform recipients that a particular event has occurred. To enable email alerts, you must have access to an active mail server.
Event classification	The categorization of events as Critical, High Medium, Low or Noise.
Event logs	A collection of entries which describe events that occurred on the network or on a computer system. GFI EventsManager supports different types of event logs including: Windows Event Log, W3C Logs, Syslog, SNMP Traps and SQL Server audit events.
Event processing rules	A set of instructions which are applied against an event log.
File and Printer sharing	Enable this firewall permission to allow GFI EventsManager to access events definitions on target machines. For more information, refer to http://technet.microsoft.com/en-us/library/cc779133(WS.10).aspx
Internet Protocol Security	A framework of open standards used to encrypt and authenticate network packets during a communication session between computers. Using cryptography services, IPsec ensures data integrity, authentication and confidentiality.
IPsec	See Internet Protocol Security

TERM	DEFINITION
Management Information Base	A MIB is the equivalent of a data dictionary or codebook. It associates object identifiers (OIDs) with a readable label and various other parameters related to an active network object such as a router. Its main function is to assemble and interpret SNMP messages transmitted from SNMP-enabled network devices. The information stored in MIBs is organized hierarchically and is normally accessible using a protocol such as SNMP.
Network alerts	Network messages (known as Netsend messages) which inform recipients that a particular event has occurred. These messages are sent through an instant messenger system/protocol and are shown as a popup in the system tray of the recipient's desktop. To setup network alerts, you must specify the name or IP of the computers where the Netsend messages will be sent.
Network discovery	Enable this firewall permission to allow GFI EventsManager to gather information about connected machines on the network that can be scanned. For more information, refer to http://technet.microsoft.com/en-us/library/cc181373.aspx
Noise	Repeated log entries which report the same event.
Object auditing	Enable this auditing feature to audit events of users accessing objects (example, files, folder and printer). For more information, refer to http://technet.microsoft.com/en-us/library/cc976403.aspx
Object auditing	Enable this auditing feature to audit tracking information (example, program activation, process exit and indirect object access). For more information, refer to http://technet.microsoft.com/en-us/library/cc775520(WS.10).aspx
Remote Event Log Management	Required to allow GFI EventsManager to access and collect events from remote machines. For more information, refer to http://technet.microsoft.com/en-us/library/cc766438.aspx
Rule-set folder	The folder which contains one or more rule-sets.
Rule-sets	A collection of event processing rules.
SMS alerts	SMS notifications which inform recipients that a particular event has occurred. In GFI EventsManager, SMS alerts can be sent through various sources including mobile phones with modem capabilities and email-to-SMS web-based gateways.
SNMP Object Identifier (OID)	An SNMP object identifier is an address made up of a sequence of 'dotted' numbers (e.g. 1.3.6.1.4.1.2682.1). These numbers uniquely identify and locate a specific device (e.g. hub) within the entire network. SNMP OIDs are a key component in the assembly of SNMP messages. In fact, an SNMP server cannot interpret or assemble messages which don't have an OID. Individual vendors often create their own MIBs that only include the OIDs associated specifically with their device.
SNMP Traps	Notifications/alerts generated and transmitted by active network components (e.g. hubs, routers and bridges) to SNMP server(s) whenever important events such as faults or security violations occur. Data contained in SNMP Traps may contain configuration, status as well as statistical information such as number of device failures to date.
Syslog messages	Notifications/alerts most commonly generated and transmitted to a Syslog server by UNIX and Linux-based systems whenever important events occur. Syslog messages can be generated by workstations, servers as well as active network devices and appliances such as Cisco routers and Cisco PIX firewalls to record failures and security violations amongst other activities.
Unclassified events	Events that did not satisfy any of the event processing conditions configured in the event processing rules.

TERM	DEFINITION
W3C logs	W3C is a common log format developed by the World Wide Web Consortium. W3C logs are text-based flat files used mainly by web servers including Microsoft Internet Information Server (IIS) to record web related events such as web logs.
Windows Event Logs	A collection of entries which describe events that occurred on a computer system running Windows OS.

Index

A

Archiving events 81, 87, 116

B

Backup events 51, 53

D

Daily Digest 1, 55, 56

Database Backend 1, 3, 5, 8, 9, 19, 23, 24, 43, 51, 81, 83, 87, 89, 116, 171, 173, 181, 186, 237

Database Operations 5, 6, 178, 181, 182, 183, 184, 185, 187, 199, 200, 202, 203, 223

Default alerting settings 146

Demilitarized Zone 15, 16

DNS server 11, 16, 102, 239

E

Email Alerts 99, 142, 145, 146, 147, 243

Event classification 5, 99, 100, 116, 142, 144, 243

Event color-coding 1, 3, 5, 35, 41

Event finder tool 1, 3, 5, 35, 43

Event processing rules 1, 3, 4, 5, 8, 78, 95, 97, 99, 116, 118, 119, 121, 122, 123, 126, 127, 130, 132, 134, 142, 172, 243, 244

Event query 3, 5, 36, 37

Events Browser 1, 3, 9, 33, 34, 36, 37, 39, 41, 43, 44, 49, 51, 52, 136, 172, 173, 174, 182

EventsManagerAdministrator 145, 153, 157

Export events to CSV 44

G

GFI EndPointSecurity 15, 95, 96, 97

GFI LANguard 93, 94, 95, 121, 173

I

Installation wizard 20, 240

L

License type 67, 233

Licensing 2, 9, 20, 68, 232, 233

Logon credentials 68, 75, 76, 80, 83, 86, 90

M

Management Information Base 6, 111, 244

N

Network alerts 8, 121, 148, 154, 243, 244

Noise Reduction 5, 121

O

Operational time 68, 76, 77, 80, 86, 125, 129, 131, 133, 135

Oracle database 4, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93

P

Performance Options 240

Q

Quick Start Dialog 24, 27, 28, 30

R

Rule-set 1, 99, 103, 118, 119, 121, 122, 123, 124, 127, 130, 132, 134, 142, 244

S

SMS alerts 148, 149, 243, 244

SNMP traps 3, 8, 13, 19, 33, 36, 68, 72, 79, 99, 110, 111, 112, 113, 121, 132, 171, 177, 179, 180, 243, 244

SQL Server audit 5, 13, 15, 33, 36, 81, 99, 121, 134, 243

Storage Folder 8, 81, 83, 103, 106, 108, 116, 181, 191, 192

Syslog messages 8, 13, 15, 17, 19, 55, 104, 106, 107, 108, 110, 130, 244

Syslog server 13, 17, 106, 107, 108, 109, 110, 171, 244

V

version information 235

W

W3C logs 4, 8, 11, 12, 68, 79, 99, 104, 105, 127, 139, 238, 243, 245

WAN Connector 5

Windows 7 17, 19, 20, 210

Windows Event Logs 4, 8, 11, 68, 99, 103, 104, 114, 118, 119, 121, 123, 124, 245

Windows Vista 17, 19, 20, 25, 34, 103, 175, 206, 211, 223